2013-12

Social media principles applied to critical infrastructure information sharing

Riccardi, Christine

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SOCIAL MEDIA PRINCIPLES APPLIED TO CRITICAL INFRASTRUCTURE INFORMATION SHARING

by

Christine Riccardi

December 2013

Thesis Advisor:	Rudolph Darken
Second Reader:	Gurminder Singh

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE SOCIAL MEDIA PRINCIPLES APPLIED TO CRITICAL INFRASTRUCTURE INFORMATION SHARING		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Christine Riccardi			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Social media is on the forefront of leading capabilities to share information faster, more broadly, and to extremely large, targeted audiences. To many in the business of disseminating information quickly to these broad audiences, social media is a critical enabler. Areas of homeland security, and in particular, critical infrastructure protection, rely significantly on sharing information with partners across the mission yet are consistently criticized for their inability or ineffectiveness at sharing information. Social media principles, the fundamentals that make social media unique and successful, may have applicability to critical infrastructure information sharing, and in turn, may further the information-sharing goals of this mission area.

This thesis explores the principles of social media, the resultant outcomes as seen in case studies with information sharing objectives similar to those in the critical infrastructure arena, and proposes applicability of those social media principles to the information sharing practices of the critical infrastructure discipline.

14. SUBJECT TERMS Critical infrastructure; Information Sharing; Social Media; Web 2.0			**15. NUMBER OF PAGES** 149
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SOCIAL MEDIA PRINCIPLES APPLIED TO CRITICAL INFRASTRUCTURE INFORMATION SHARING

Christine Riccardi
Deputy Chief of Staff, Department of Homeland Security, National Programs Protection Directorate, Office of Infrastructure Protection, Arlington, VA
B.S., University of Dayton, 2003
M.S., Johns Hopkins University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Christine Riccardi

Approved by: Rudolph Darken, PhD
Thesis Advisor

Gurminder Singh, PhD
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Social media is on the forefront of leading capabilities to share information faster, more broadly, and to extremely large, targeted audiences. To many in the business of disseminating information quickly to these broad audiences, social media is a critical enabler. Areas of homeland security, and in particular, critical infrastructure protection, rely significantly on sharing information with partners across the mission yet are consistently criticized for their inability or ineffectiveness at sharing information. Social media principles, the fundamentals that make social media unique and successful, may have applicability to critical infrastructure information sharing, and in turn, may further the information-sharing goals of this mission area.

This thesis explores the principles of social media, the resultant outcomes as seen in case studies with information sharing objectives similar to those in the critical infrastructure arena, and proposes applicability of those social media principles to the information sharing practices of the critical infrastructure discipline.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APTA	American Public Transit Association
CHDS	Center for Homeland Security and Defense
CI	Critical Infrastructure
CI ISE	Critical Infrastructure Information Sharing Environment
CIPAC	Critical Infrastructure Protection Advisory Council
CVI	Chemical-terrorism Vulnerability Information
DARPA	Defense Advanced Research Project Agency
DHS	Department of Homeland Security
DoS	Department of State
GAO	Government Accountability Office
GTRI	Georgia Tech Research Institute
HSIN-CS	Homeland Security Information Network—Critical Sectors
IC	Intelligence Community
IP	Infrastructure Protection
ISAC	Information Sharing and Analysis Centers
ISARB	I Spy a Red Balloon
ISWG	Information Sharing Working Group
NCRIC	Northern California Regional Intelligence Center
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
OECD	Organisation for Economic Co-operation and Development
OCIO	Office of the Chief Information Office
PCII	Protected Critical Infrastructure Information
PISA	Programme for International Student Assessment
PSA	Protective Security Advisor
PT-ISAC	Public Transportation Information Sharing and Analysis Center
QHSR	Quadrennial Homeland Security Review
SCP	Service Chief's Program
SOP	Standard Operating Procedures
SSA	Sector Specific Agency
SSI	Sensitive Security Information

TSA	Transportation Security Agency
UCC	User Created Content

EXECUTIVE SUMMARY

Social media is on the forefront of leading capabilities to share information faster, more broadly, and to extremely large, targeted audiences. To many in the business of disseminating information distributed quickly to these broad audiences, social media is a critical enabler. However, some fields have been slower to adopt it than others. Areas of homeland security, and in particular, critical infrastructure protection, rely significantly on sharing information with partners across the mission. Moreover, homeland security missions are consistently criticized for their inability or ineffectiveness at sharing information. Social media principles, the fundamentals that make social media unique and successful, may have applicability to critical infrastructure information sharing, and in turn, may further the information sharing goals of this mission area.

The Critical Infrastructure Information Sharing Environment (CI ISE) is the structural framework that enables the Department of Homeland Security (DHS) to share infrastructure protection information with its key partners. Critical infrastructure partners, governments, regulators, and advisors agree that information sharing has significant room for improvement, especially as it is the most integral piece of the mission.[1] Criticism and recommendations for improvement center around the value of the information delivered within the environment, the totality of the stakeholder membership, timeliness of delivery, and the nature of multi-directional collaboration between stakeholders.[2]

Putting aside the public social media technologies, the principles that make social media successful have applicability to critical infrastructure information, and in turn, may further the information sharing goals of this mission area and address the known deficiencies. Principles, such as group-based collaboration, group-based collection, casual communication, direct communication, network self-selection, and tagging, can be

[1] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 2012; U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach* (2010), 57; U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing* (2011).

[2] Ibid.

attributed to successful information sharing outcomes when applied to practical scenarios. Outcomes experienced in other applications are similar to those required by the CI ISE to achieve its intended function and mitigate the shortcomings cited by the National Infrastructure Advisory Council (NIAC) and others.[3]

To answer the question of how social media principles may be applied to critical infrastructure information sharing, and in turn, how those principles may improve information sharing, three case studies in which social media principles have been applied to share information reveal evidence that the studies' successful outcomes would present in the CI ISE if the same principles were applied. Social media principles are the characteristics and capabilities found in modern web applications that drive effective information sharing on the tools they are employed within. Among the three studies, 13 common and prevalent social media principles are cataloged, each having utility in information-sharing environments. It is important to note that these principles are not the tools themselves. In other words, Twitter is a branded information technology that enables quick, direct, and casual communication in a public forum. The social media principles employed by Twitter are such characteristics as casual communication and direct communication.

The first case study—the Defense Advanced Research Project Agency (DARPA) Network Challenge—demonstrates the use of crowdsourcing to achieve an objective to locate 10 geographically diverse locations.[4] The challenge—ultimately a contest—revealed strategies and approaches that top competitive teams employed to compete in the challenge. These strategies included many diverse applications of social media principles. The results of the challenge show considerable utility for principles beyond crowdsourcing, such as the ability for an individual to choose and join a network and direct communication.

The Department of State's (DoS) Office of eDiplomacy aims to combine diplomacy with collaborative technology by creating an innovated approach to

[3] National Infrastructure Advisory Council, *Intelligence Information Sharing*.

[4] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*, 2010.

knowledge sharing and supreme customer service.[5] eDiplomacy consists of several homegrown tools and information sharing platforms that employ a number of social media principles. The closed network fosters a protected information-sharing environment while still leveraging modern capabilities for collaboration.

Finally, the third case study presents examples from across the globe, where with the assistance of success information sharing strategies, the education system in Rio de Janeiro was transformed. Somewhat by accident, Claudia Costin, the Secretary of Education, began collaborating publically with her teacher community. It did not take long for the conversation to be enriched with a multi-way dialogue and soon other collaboration platforms emerged. Among them, Rio de Janeiro employed both public and private tools to ensure that the entire educational community had an opportunity to obtain and share information. Each platform took advantage of social media principles, such as group-based collaboration, direct communication, and dynamic editing. Ultimately, the education system celebrated the success of reform that can be attributed to the enriched conversations that resulted from the information-sharing platforms powered by the social media principles.

Each case study was analyzed for outcomes attributed to one or more of the 13 social media principles. The outcomes seen in the studies are similar to the objectives and goals of the CI ISE. The case studies reviewed in this thesis represent a variety of goals intended to be met with information-sharing mechanisms. While none of these goals is specific to homeland security or the critical infrastructure protection and security missions, they have other attributes in common with the CI ISE. Most notably, these case studies produced outcomes that mirror outcomes expected to be achieved through the CI ISE when the characteristics are well functioning and effective. Also, the case studies applied their social media principles across open and closed environments, which is representative of how critical infrastructure information is to be shared. The evidence and analysis resulting from three cases, their outcomes, related use of social media principles, and ultimate mapping to the CI ISE, suggest that applying the social media principles will

[5] U.S. Department of State, "IRM's Office of eDiplomacy," (n.d.), http://www.state.gov/m/irm/ediplomacy/.

have utility in the CI ISE. Further, because many of the characteristics described for the CI ISE are actually documented shortcomings, the principles related to those characteristics may improve the CI ISE when applied in those areas.

The case studies reviewed are only a small sample set of information-sharing problems that have been addressed with the application of modern information-sharing practices, such as social media. The case studies reviewed had 113 applications that would impact the CI ISE. It is reasonable to conclude that even more evidence would be found that further substantiates the applicability of social media principles to the CI ISE.

Due to the nature of the critical infrastructure protection and security, and its requirement for secure exchange of information, it is important that any consideration towards applying social media principles does not equate to using public forums to share information. The three case studies presented in this thesis all demonstrated application of the principles distinct from common and well-known social media technologies. The DARPA Network Challenge teams used some public tools, such as Twitter and Facebook, but also took advantage of other less public facing networks. The Rio de Janeiro case exemplified using both public social media tools, as well as closed environment solutions. Twitter was a catalyst to starting the conversation and creating the network from which the reform efforts were able to launch more closed conversations and joint efforts. Social media principles were applied to the closed environments, like Educopédia and "Fala, Professor!," to achieve a similar environment to public social media tools. Finally, the DoS eDiplomacy case demonstrated application of social media principles completely within a closed, non-public environment. While the suite of tools mimics popular social media tools, the application of the principles was completely divorced from using public tools. Based on the cased studies' successful application of social media principles absent the use of social media public technologies, the CI ISE can expect to achieve a similar implementation strategy, while maintaining and protecting the integrity and sensitivity of the information in the environment.

As noted in the case study summaries, the case studies used various technologies to employ the social media principles. While the DARPA Network Challenge took advantage of readily available technologies, mostly public networking tools, the DoS

built homegrown tools, and the Rio de Janeiro environment used a mix. This mix of implementation approaches underscores that social media principles, when applied, achieve the information-sharing outcomes desired in the CI ISE, regardless of the technology that employs the principle, including publically accessible technology.

In conclusion, the environment can be improved, and some of the issues and shortcomings found by the NIAC Intelligence Information Sharing study and others, will be addressed by applying social media principles—those features and characteristics that make social media rich with information and networks—to the technologies that support the environment.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Thank you to my friends and family for the support, encouragement, and patience while I worked toward completing this program and this thesis. You never tired of my excuses that I was “working on my thesis” instead of joining you in various, likely more fun, activities. Your endless support made each milestone that much more meaningful. Thank you.

Thank you to my work family at the Office of Infrastructure Protection, who encouraged my participation throughout the program and found interest in my studies for the betterment of our organization.

Thank you to my thesis committee, Rudy and Gurminder, who provided guidance along the way, and validation and confirmation I was on the right track. Your counsel and time are very appreciated and reflected in this thesis.

To the staff and faculty of the Center for Homeland Defense and Security (CHDS)—thank you for contributing to a second-to-none graduate school experience. I am grateful today, and forever, for the opportunity to grow and learn with your support and leadership. You are part of a first class program, and I am so honored to have journeyed with you.

Finally, to each and every one of my classmates of 1203/1204, I will remain in awe of the amount of courage, intelligence, knowledge, and integrity each of you brought to CHDS and to my personal learning experience and journey. I have made lasting friendships with you that I look forward to fostering for years to come. Without a doubt, my classmates made the CHDS experience far exceed all imaginable expectations. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

On September 21, 2013, the shopping day of shoppers and mall employees typical was gravely disrupted. On this day, gunman launched gunfire attacks on the Westgate shopping mall in Nairobi, Kenya. The attack persisted for four days, which finally concluded on September 24 with a total of 72 fatalities. The Islamist group al-Shabaab claimed responsibility for the incident. As Americans watched and waited for the situation to unfold, the United States retail industry started preparing for appropriate security measures given the overseas tragedies. The Department of Homeland Security (DHS) urged its retail industry partners to heighten security and reminded them of the precautions when dealing with active shooters.

The DHS works throughout the year to build partnerships with industries across a wide spectrum, to include commercial facilities. They provide information to these partners when a specific threat is known or when a reason exists for heightened awareness. Along with threat information, the DHS provides partners protective measures, potential indicators, and common vulnerabilities to help industries maintain the good security postures.

The Nairobi incident had DHS officials immediately sharing situational updates and guidance to industry, primarily via teleconferences and meetings. Information was also shared on secure information sharing portals. However, with a retail industry that includes over 3.6 million establishments, and has sales of over $2.5 trillion, are those information sharing measures enough?[1] Are they reaching all the intended establishments? Has the industry, either domestic or abroad, already taken effective measures against the impending threat? What are other measures that similar retail institutions are implementing? These questions and more are challenging to answer with one-way pushes of information and little opportunity for collaboration.

[1] SelectUSA, "The Retail Services Industry in the United States," (n.d.), http://selectusa.commerce.gov/industry-snapshots/retail-services-industry-united-states.

This thesis explores the use of social media principles, applied to the current information sharing environment for critical infrastructure, to answer these sorts of questions.

A. RESEARCH QUESTION

Social media is on the forefront of leading capabilities to share information faster, more broadly, and to extremely large, targeted audiences. To many in the business of disseminating information quickly to these broad audiences, social media is a critical enabler. Yet, some fields have been slower to adopt it than others. Areas of homeland security, and in particular, critical infrastructure protection, rely significantly on sharing information with partners across the mission. Moreover, homeland security missions are consistently criticized for their inability or ineffectiveness at sharing information. Social media principles, the fundamentals that make social media unique and successful, may have applicability to critical infrastructure information sharing, and in turn, may further the information sharing goals of this mission area.

The research question for this thesis is the following.

> Can social media principals be applied or added to the U.S. approaches to sharing information for critical infrastructure protection for an improved experience and outcome?

This research question will be investigated by (1) clearly defining "social media principles" to focus on application to the DHS mission, (2) describe how the unique characteristics of social media map onto stated DHS information sharing objectives, (3) develop metrics that measure added value of social media in this domain, and (4) apply these metrics to case studies to demonstrate utility of social media for information sharing in critical infrastructure protection.

B. PROBLEM SPACE

The *Quadrennial Homeland Security Review* (QHSR) outlines the protection of the Nation's Critical Infrastructure as a key strategic mission area for the DHS.[2] To

[2] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review* (Washington, DC: U.S. Department of Homeland Security, 2010).

execute this mission, the DHS is responsible for the protection and resilience of the nation's critical infrastructure. Without regulatory authority over infrastructure, which is predominately owned and operated by private industry and regulated by government organizations outside of the DHS, it achieves this mission by influencing voluntary risk management programs. These programs rely significantly on sharing information, bi-directionally, between government and industry partners. The diversity of partners within the critical infrastructure community makes it necessary for a framework and structure to ensure information flows among partners to achieve coordination, communication, and collaboration in reducing risk to the nation's infrastructure.[3]

The Critical Infrastructure Information Sharing Environment (CI ISE) is the structural framework that enables the DHS to share infrastructure protection information with its key partners. Critical infrastructure partners, governments, regulators, and advisors agree that information sharing has significant room for improvement, especially as it is the most integral piece of the mission.[4] Criticism and recommendations for improvement center around the value of the information delivered within the environment, the totality of the stakeholder membership, timeliness of delivery, and the nature of multi-directional collaboration between stakeholders.[5]

In contrast to the information-sharing effectiveness within the critical infrastructure mission area, social media technologies are embedded in the day-to-day operations throughout the world, among all generations and walks of life. No longer a subject just for young technology enthusiasts, today, many interact with social media on a daily and even hourly basis. Facebook is a notable example of this type of information-sharing technology that to date has over 955 million users worldwide.[6] Twitter, a close

---

[3] U.S. Department of Homeland Security, *Critical Infrastructure Key Resources Information Sharing Environment White Paper* (Washington, DC: U.S. Department of Homeland Security, 2012).

[4] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 2012; U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach* (2010), 57; U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing* (2011).

[5] Ibid.

[6] Facebook Newsroom, "Key Facts," 2013, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

rival for most-used technology of this kind, hosts over two million tweets a day.[7] The impact on the way information is shared through many aspects of modern life is undisputable. Businesses have changed their models and leveraged this technology to market to new customers, provide competitive services, and appeal to modern requirements for information. What social media technologies have in common is a fundamental set of principles, which drive the application and effectiveness of the tools that embody them.

Meanwhile, in the context of homeland security, the pace to embrace these same exploding phenomena realized in social media applications is noticeably not as swift. Governments across all levels battle the advantages of using social media with the challenges and risk the same technologies present. It is often the case that the very idea of social media becomes synonymous with specific tools. The idea of using Facebook or Twitter to share sensitive security information is perplexing to governments and rightfully so. The protection, security, and resilience of critical infrastructure requires sharing sensitive information, such as intelligence information regarding emerging threats, tactics and techniques, and particulars about individual assets and their vulnerabilities and risks to all-hazard events. The sensitive nature of this information requires secure information sharing, opposed to sharing in public venues and forums. Consequently, the same reluctance is experienced throughout the government to embrace social media. Moreover, the distinction between using public social media technologies and embracing the modern techniques these technologies employ is lost in the concern for ensuring that information is shared securely.

Putting aside the public social media technologies, the principles that make social media successful may have applicability to critical infrastructure information, and in turn, may further the information-sharing goals of this mission area and address the known deficiencies. Principles, such as group-based collaboration, group-based collection, casual communication, direct communication, network self-selection, and tagging, can be attributed to successful information-sharing outcomes when applied to practical

[7] Twitter Stats, "TweetStats," 2013, http://www.tweetstats.com//twitter_stats.

scenarios. Outcomes experienced in other applications are similar to those required by the CI ISE to achieve its intended function and mitigate the shortcomings cited by the National Infrastructure Advisory Council (NIAC) and others.[8] The proposed topic explores the theories, principles, and underpinnings of social networking and discovers if application to the critical infrastructure information sharing would yield a more robust, comprehensive result than current information-sharing practices.

C. STRUCTURE AND SUMMARY OF CASE STUDY METHOD

To answer the question of how social media principles may be applied to critical infrastructure-information sharing, and in turn, how those principles may improve information sharing, this thesis reviews and analyzes three case studies where social media principles have been applied to share information. Social media principles are the characteristics and capabilities found in modern web applications that drive effective information sharing on the tools they are employed within. This thesis catalogs 13 common and prevalent social media principles by describing their utility in information-sharing environments. It is important to note that these principles are not the tools themselves. In other words, Twitter is a branded information technology that enables quick, direct, and casual communication in a public forum. The social media principles employed by Twitter are such characteristics as casual communication and direct communication. Social media principles are described in detail in Chapter V.

Each case study is summarized and described for the overarching goals each scenario aimed to achieve. In the process of achieving those goals, each case study scenario demonstrated several information-sharing outcomes. The outcomes from these case studies are attributed to social media principles catalogued in Chapter V. Since the focus of the central question is the principles of social media, not the media itself, studies were reviewed for the fundamental aspects employed to successfully or unsuccessfully achieve the objective level of information sharing. The resulting data construct includes three case studies, the outcomes observed in these studies, and the associated principles that enabled the outcomes.

[8] National Infrastructure Advisory Council, *Intelligence Information Sharing*.

Meanwhile, the CI ISE has been evaluated for general goals and objectives in support of the critical infrastructure protection and security mission. Additionally, the reported and documented shortcomings and areas for improvement are coupled with the main objectives of the CI ISE, which resulted in four categories of desired and intended characteristics of the environment. These characteristics serve as the basis by which social media principles may be applied to improve the CI ISE achievement of successful information sharing in support of a voluntary risk management.

The case study outcomes are compared to each characteristic desired in the CI ISE. When an outcome of a case study yielded an information-sharing success similar to what intended by the CI ISE characteristic, a match is recorded. This next level of data compilation now includes several outcomes mapped to each characteristic. Then , the same social media principles responsible for the case study outcomes are mapped to each CI ISE characteristic associated with a particular outcome. The identified critical infrastructure information-sharing characteristic areas are reevaluated with the principle outcomes from the case studies to predict potential improvement in the critical infrastructure environment. Principles that have apparent merit for improving information sharing are offered as recommended areas for implementation.

1. Case Study Selection

Many examples exist to show how social media has been applied against information-sharing objectives geared towards sharing information with the public, including government and security agencies. However, because information sharing among the critical infrastructure community is typically sensitive and shared in a closed network, case studies that have used social media in a less traditional way than public information sharing were considered for review and explored further. Studies in which information is exchanged bi-directionally, and between government and non-government stakeholders, are best poised to answer this question.

Case studies were reviewed from the literature, trade publications, government reports and similar items found in academic and government publications. Ideal studies include the key characteristics of sharing information in the critical infrastructure

community, such as sensitive, security information, large geographic and industry diverse stakeholder sets, emergency, incident and steady state operations, and diverse virtual environments. Each case study considered was reviewed for basic characteristics, such as the following.

- How social media was used to share information
- The information-sharing objectives
- The stakeholder composition on both sides of the information exchange (i.e., government/non-government, consumers, authors)

Specific case studies have been chosen to explore areas in which challenges in critical infrastructure information sharing have made adopting new media a less obvious progression. Case studies are considered for timeliness of information, quality and accuracy of content, expansive reach, private networks, and sharing sensitive information.

2. Case Study I: DARPA Network Challenge

In 2009, the Defense Advanced Research Project Agency (DARPA) challenged the public with what came to be a significant exemplar of crowd sourcing and the power of social media in a distributed challenge. The DARPA Network Challenge intended to demonstrate how a geo-diverse challenge could be solved by crowdsourcing.[9] This case study reviews the details of the contest objectives and understands several competitive team strategies for crowdsourcing the information required to win the contest. The case study revealed a diverse set of outcomes stemming from six different social media principles.

3. Case Study II: Department of State's eDiplomacy

The DoS's Office of eDiplomacy aims to combine diplomacy with collaborative technology to create an innovative approach to knowledge sharing and superior customer service.[10] Due to the nature of constantly rotating assignments by State office personnel,

[9] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*, 2010.

[10] U.S. Department of State, "IRM's Office of eDiplomacy," (n.d.), http://www.state.gov/m/irm/ediplomacy/.

the DoS is naturally challenged to manage, maintain, and organize institutional knowledge. At the same time, it is charged with ensuring that officers on new duty assignments have the information necessary to meet the objectives of their assignments successfully, and in short order of onboarding. The office was created to meet these objectives. It uniquely combines innovative technology with diplomacy and provides the DoS' employees with a variety of tools and resources to achieve these improved knowledge-sharing and communication goals. This case study highlights four of these tools and outlines how social media principles have contributed to the overarching information sharing goals of the eDiplomacy office, which reveals 15 outcomes using eight social media principles.

4. Case Study III: Rio de Janeiro Education Reform

Since the mid 1990s, Brazil has experienced tremendous and impressive growth in the quality and results in their education system. The rise of education in Brazil has been the fastest on record, second only to China, and the country is considered a global leader in assessing student learning and education performance monitoring.[11] Nevertheless, despite the major improvement trends over the last 15 years, as recently as 2009, student proficiency in key subjects, such as math, is still averaging far below member countries of the Organisation for Economic Co-operation and Development (OECD).[12] Claudia Costin became the secretary of education for the municipality of Rio de Janeiro in 2008. She inherited an education system that, while improving, was still plagued with below average scores and proficiencies of OECD and like countries.[13] This case study explores how Costin employed a strategy to build trust with teachers, largely through the transparency of social media, to turn the education system around. Unique to

[11] Barbara Bruns, David Evans, and Javier Luque, *Achieving World-Class Education in Brazil: The Next Agenda* (Washington, DC: World Bank, 2011), 3.

[12] OECD presently has 34 member countries and was founded to stimulate economic progress and world trade. Education is a main policy area the organization contributes to. OECD, "Organisation for Economic Co-Operation and Development," 2013, http://www.oecd.org/general/organizationforeuro peaneconomicco-operation.htm.

[13] Bruns, Evans, and Luque, *Achieving World-Class Education in Brazil: The Next Agenda*, 25.

this study, Costin's education reform was successful using both public and close-network information-sharing environments. The study outlines 14 outcomes that used nine different social media principles.

D. OVERVIEW OF UPCOMING CHAPTERS

The second chapter provides a literature review of current publications and available research concerning the subjects of social media principles, the current practices of sharing information within the critical infrastructure community, and applicability of social media to the homeland security mission.

Following, the next chapters provide background and foundation for both critical infrastructure and its information-sharing practices and social media principles. Chapter III discusses in further detail how the critical infrastructure owners and operators collaborate and receive information from their government partners. The chapter also summarizes notable reviews of the current state of information sharing, outlining areas recommended for improvement.

Meanwhile, Chapter IV describes 13 common principles responsible for the effectiveness of social media platforms and tools. These principles are later correlated to successes found in three case studies.

The case studies are described for background in Chapter V, followed by an understanding of how each study embraced one or more social media principle. This chapter relates the use of each principle to information sharing outcomes achieved in each study.

Chapter VI tabulates the outcomes found in the case studies with the desired improvements and objectives of the CI ISE. The chapter describes the relationship between the outcomes, the desired CI ISE objectives, and the use of social media principles.

The final chapter, Chapter VII, describes a model whereby the principles studied in this thesis could affect the successful execution of desired outcomes of the CI ISE, if applied. The chapter concludes by describing likely impediments to executing such a model and outlines basic implementation plans for integrating social media principles in the CI ISE.

II. LITERATURE REVIEW

Protecting and ensuring a resilient critical infrastructure is a mission area achieved mostly in a voluntary environment, as private industry owns and operates most of the nation's critical infrastructure. To affect this mission, government agencies and departments rely significantly on sharing information, bi-directionally, between government and industry partners. The DHS has established the CI ISE as a framework for achieving this component of the protection and security mission. The framework includes a diverse set of mechanisms, policies, and information types for sharing information. However, opportunities to improve information-sharing mechanisms and quality—and therefore the effectiveness of information shared—have been identified by a number of sources.[14]

A literature review has revealed material on approaches and practices to information sharing with critical infrastructure stakeholders. In addition to the approaches and practices of critical infrastructure information sharing, the review yielded documented criticisms and shortcomings with respect to the outcomes and effectiveness of the information-sharing portion of the critical infrastructure mission.

In recent years, social media is a growing trend in information sharing and has also emerged in applications for homeland security. Social media is a collection of capabilities and technologies that make a network of user-created content possible. Notable and popular examples of social media tools include social networking sites, such as Facebook and Twitter, video sharing, such as YouTube and Vimeo, picture sharing, such as Shutterfly and Piascso, combination network and media sites, such as Instagram, collaboration projects like *Wikipedia*, and virtual gaming and social words, such as World of Warcraft and Second Life. These examples represent tools that employ the concepts and principles of social media and are not in themselves social media. The literature review informed definitions categorical of social media capabilities—or principles—

[14] See National Infrastructure Advisory Council, *Intelligence Information Sharing*; U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*; U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

responsible for implementing the tenets of modern information sharing and Web 2.0. In addition to the principles of social media, the review found several case studies that illustrate the use of these principles and associated information-sharing outcomes that resulted.

The scope of this review discusses available literature in four areas: 1) strategic plans and policies describing the framework for critical infrastructure information sharing, 2) reviews of critical infrastructure information sharing, including shortcomings and criticisms, 3) social media principles, and 4) case studies in which these principles have been implemented.

A. CRITICAL INFRASTRUCTURE INFORMATION SHARING

The DHS is charged with leading this mission but must succeed with participation from both public and private stakeholders of the critical infrastructure community. Presidential Policy Directive-21, Critical Infrastructure and Resilience, outlines the federal strategy for protecting infrastructure and the responsibilities of the federal government against that mission.[15] A derivative from the previous Homeland Security Presidential Directive-7, the *National Infrastructure Protection Plan* (NIPP) implements the federal strategy and describes a nationwide approach with a voluntary emphasis on critical infrastructure security and resilience.[16] All these doctrine provide emphasis on information sharing, its importance, and introduces the CI ISE as the framework for doing so.

The CI ISE is the primary private sector component of the National Information Sharing Environment. The environment itself is not a tangible system, network, or program, but rather is a collection of frameworks, policies, governance structures, and implementation systems that collectively contribute to the goal of sharing information between critical infrastructure stakeholders. The *Critical Infrastructure Information*

[15] The White House, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[16] Michael Chertoff, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security (DHS), 2009).

Sharing Environment paper describes the framework for sharing information between the public and private sector within the critical infrastructure environment.[17] The framework, comprised of various components and facets, is designed to provide a flexible and adaptable set of mechanisms by which the critical infrastructure stakeholder set can share information effectively.

As a unifying framework, CI ISE is purposed to include and leverage capabilities for information sharing across the enterprise and not rely solely on one specific technology mechanism. Where possible, information is delivered into the Homeland Security Information Network—Critical Sectors (HSIN-CS) portal environment via feeds and other interoperable capabilities. Additionally, however, other technologies are included in the CI ISE, even if they do not technically interoperate. The paper notes distinctly that the totality of the CI ISE includes other mechanisms, some of which are difficult to define, track, and measure. The paper does not include details on the various capabilities within any one technology, nor does it explore information-sharing strategies accomplished specifically with capabilities. Social media or new media is not addressed.

B. CURRENT SHORTCOMINGS AND GAPS

Despite the framework designed for implementation, the CI ISE is reported in literature to fall short of achieving its full potential. Criticism and recommendations for improvement center around the value of the information delivered within the environment, the totality of the stakeholder membership, and the nature of multi-directional collaboration between stakeholders. The NIAC issued a report in January 2012 on intelligence information sharing.[18] The NIAC's study included the CI ISE and HSIN-CS, which is the primary implementation technology for the CI ISE. The study revealed areas in which the CI ISE was successful at delivering valuable content and serving as an information hub. It also outlined a number of areas for improvement across content, usability, and reach. The Government Accountability Office (GAO) has also

[17] U.S. Department of Homeland Security, *Critical Infrastructure Key Resources Information Sharing Environment White Paper*.

[18] National Infrastructure Advisory Council, *Intelligence Information Sharing*.

conducted studies and reports that address the effectiveness of critical infrastructure information sharing. The GAO found in its Rail Security Study that the rail sector's multiple information platforms compete for stakeholder attention and none of those platforms was reaching an adequate stakeholder share.[19] Similarly, the September 2010 GAO report on Public Transit Security Information Sharing identified many different mechanisms for the rail industry to receive infrastructure security information and found that most industry members use at least five mechanisms collectively to receive information.[20] Multi-directional collaboration in the CI ISE is achieved when stakeholders interact as consumers and contributors to the environment, ideally on the same content. All three of these reports and studies found shortcomings with multi-directional collaboration.

C. SOCIAL MEDIA PRINCIPLES

Web 2.0 technologies refer to the second generation of the World Wide Web, in which paradigms for online information delivery shifted to capabilities and user experiences that offer user participation and promote collaboration through user-generated content.[21] Tim O'Reilly popularized the term Web 2.0 at the inaugural Web 2.0 conference in 2004 and his web article on the subject served as a baseline for understanding the principles that embody both Web 2.0 and social media.[22] Kaplan and Haenlein dedicate a brief but thorough journal article to understanding the various categories of social media, based on the Web 2.0 foundation.[23] Kaplan and Haenlein categorize social media into six categories: 1) collaborative projects, 2) blogs and microblogs, 3) content communities, 4) social network sites, 5) virtual game worlds, and

---

[19] U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*.

[20] U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

[21] *Wikipedia*, s.v. "Web 2.0," last modified November 28, 2013, http://en.wikipedia.org/wiki/Web_2.0.

[22] Tim O'Reilly, "What Is Web 2.0," *O'Reilly Media*, 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

[23] Andreas M. Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons* 53, no. 1 (2010): 59–68.

6) virtual social words.[24] These categories are not mutually exclusive; in other words, more than one of each category are often exemplified in single social media application. Dynamic content editing is a fundamental principle of collaborative projects, of which *Wikipedia* is a notable technology example. In addition to *Wikipedia*'s own historical account on its website, Ori Brafman and Rod Beckstrom account the phenomena of the online, group-authored resource in *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations.*[25] Jim Giles' journal article on the accuracy of group-based composition provided credence to the utility and effectiveness of *Wikipedia* and other similar applications of the dynamic content editing principle.[26]

Wikipedia's article, "Social Bookmarking" as well as the D-Lib Magazine journal article reviewing social bookmarking, informed group-based collection.[27] Scott Golder and Bernardo Huberman in "The Structure of Collaborative Tagging Systems" described the common principle of tagging.[28] Meanwhile, Jame Surowiecki analyzed collective wisdom versus the wisdom of any one group member. His theories, combined with definitional information from *Wikipedia* and the Crowdsourcing TypePad blog, scoped the content for the crowdsourcing principle.[29] Social networking sites that include the principles of personal user profiles, choose your own network, direct communication and casual communication, were informed by the Nielson Company report on the state of social media and a historical review of social networking found in the *Journal of*

---

[24] Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," 59–68.

[25] *Wikipedia*, s.v. "About," last modified November 27, 2013, http://en.wikipedia.org/wiki/; Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York, NY: Penguin, 2006).

[26] Jim Giles, "Internet Encyclopaedias Go Head to Head," *Nature* 438, no. 7070 (2005): 900–901.

[27] *Wikipedia*, s.v. "Social Bookmarking, last modified October 29, 2013, http://en.wikipedia.org/wiki/Social_bookmarking; Tony Hammond et al., "Social Bookmarking Tools (I) a General Review," *D-Lib Magazine* 2, no. 4 (2005).

[28] Scott Golder and Bernardo A. Huberman, "Usage Patterns of Collaborative Tagging Systems," *Journal of Information Science* 32, no. 2 (2006): 198–208.

[29] James Surowiecki, *The Wisdom of Crowds* (New York, NY: Random House Digital, Inc., 2005); *Wikipedia*, s.v. "Crowdsourcing," last modified November 28, 2013, http://en.wikipedia.org/wiki/Crowdsourcing; Crowdsourcing, "Crowdsourcing: A Definition," June 2, 2006, http://crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html.

Computer-Mediated Communication.[30] Throughout the review of social media principles, well-known public social media technology sites served as resources for understanding the principles and their utility. Twitter, Facebook, Delicious, *Wikipedia*, Ushahidi, and Google+ were all referenced directly.[31]

D. SOCIAL MEDIA CASE STUDIES

Examples and case studies demonstrating utility of social media principles are prevalent across literature. Many examples exist of how social media has been applied against information sharing objectives geared towards sharing information with the public, including government and security agencies. Case studies were reviewed from literature, trade publications, government reports, and similar items found in academic and government research. Ideal studies include the key characteristics of sharing information in the critical infrastructure community, such as sensitive, security information, large geographic and industry diverse stakeholder sets, emergency, incident and steady state operations, and diverse virtual environments.

The first case study—the Defense Advanced Research Project Agency (DARPA) Network Challenge—is described in the *DARPA Network Challenge Report*, published the year after the contest in 2010.[32] The report outlines the objectives of the challenge, which informed the objectives to study as information-sharing objectives in the case study. The report also discussed the strategies and approaches the top competitive teams employed to compete in the challenge. These strategies included many diverse

[30] The Nielsen Company, "State of Media: The Social Media Report," December 4, 2012, http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf; Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210–230.

[31] Twitter Stats, "Popular Apps and Tweets," (n.d.), http://tweetstats.com/twitter_stats; Facebook Newsroom, "Key Facts"; Delicious, "About Us," (n.d.), https://delicious.com/about; *Wikipedia*, s.v. "About," last modified November 27, 2013, http://en.wikipedia.org/wiki/Wikipedia:About; Ushahidi, "Ushahidi," (n.d.), http://ushahidi.com/; Official Blog, "Google+: Communities and Photos," December 6, 2012, http://googleblog.blogspot.com/2012/12/google-communities-and-photos.html.

[32] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

applications of social media principles. Meanwhile, news articles covering the contest as it unfolded (December 2009) also provided valuable insight into the various ways in which the contest was participated.[33]

The DoS's Office of eDiplomacy aims to combine diplomacy with collaborative technology to create an innovated approach to knowledge sharing and supreme customer service.[34] Its website describes most of the initiatives and platforms within the eDiplomacy suite. Reviews of the "About" pages for Diplopedia , Communities @ State, and the Corridor on the DoS's public website provided a description of the various collaboration and information-sharing capabilities.[35] Social media principles used were extracted from these descriptions. Meanwhile, a conference paper on the engineering challenges related to implementing Diplopedia revealed a deeper understanding of the application of social media, and Lowry Institute for International Policy's report on the spread of eDiplomacy, presented context for application of the online collaboration suite into the international Foreign Service world.[36]

The third case study emerged from William Bratton and Zachary Tumin's *Collaborate or Perish!: Reaching Across Boundaries in a Networked World*. In their book, the education reform of Rio de Janeiro was described as an example of the power of collaboration towards progress and change.[37] This book described some of the catalysts for change, which include information sharing across several platforms. Barbara Burns, David Evans, and Javier Luque contributed to the paper, "Achieving World Class

---

[33] CNN.Com, "MIT Wins $40,000 Prize in Nationwide Balloon-Hunt Contest," December 7, 2009, http://www.cnn.com/2009/TECH/12/05/darpa.balloon.challenge/index.html?_s=PM:TECH.

[34] U.S. Department of State, "IRM's Office of eDiplomacy."

[35] Ibid.; U.S. Department of State, "About: Diplopedia," October 12, 2012, http://www.state.gov/m/irm/ediplomacy/115847.htm; U.S. Department of State, "Major Programs of IRM's Office of eDiplomacy," (n.d.), http://www.state.gov/m/irm/ediplomacy/c23840.htm.

[36] Chris Bronk and Tiffany Smith, "Diplopedia Imagined: Building State's Diplomacy Wiki," in *Proceedings of the 2010 International Symposium on Collaborative Technologies and Systems* (Chicago, IL: IEEE, 2010), http://bakerinstitute.org/files/824/; Fergus Hanson, *Revolution@ State: The Spread of eDiplomacy* (Sydney NSW 2000 Australia: Lowy Institute for International Policy, 2012).

[37] William Bratton and Zachary Tumin, *Collaborate Or Perish!: Reaching Across Boundaries in a Networked World* (New York, NY: Random House Digital, Inc., 2012).

Education in Brazil: The Next Agenda" for the World Bank.[38] This paper provided context for the education reform happening across Brazil and some of the specifics related to the progress in Rio. These items, coupled with online artifacts of the collaboration, such as the Educapedia website, provided the methods and strategies that employed social media principles for review.[39]

The OECD's website provided an understanding of how schools and youth populations are measured in education across the globe.[40] The OECD operates the Programme for International Student Assessment (PISA) study, which evaluates 15-year old student scholastic performance in math, science, and reading.[41] It was first conducted in 2000 and is repeated every three years. It is designed to assess impact of education quality on income and for understanding achievement differences between nations.[42] These materials provided an understanding of the benchmark, which the case study ultimately showed was surpassed through online collaboration.

E. REVIEW

The research gathered for this literature review revealed a diverse documentation set for the U.S. approach to information sharing with critical infrastructure, the shortcomings of those approaches, as well as other strategies across the globe. The literature is diverse and plentiful in strategies, plans, and policies that describe information sharing for critical infrastructure. However, these documents do not address specific information sharing capabilities used to achieve information sharing effectively. The review of operational examples of information sharing included both tools and social media and while many literature pieces describe operational examples in homeland security, they do not address social media and the related principles directly applied to

---

[38] Bruns, Evans, and Luque, *Achieving World-Class Education in Brazil: The Next Agenda*.

[39] Educopédia, "Educopédia," (n.d.), http://www.educopedia.com.br/SobreEducopedia.aspx.

[40] OECD, "Organisation for European Economic Co-Operation," (n.d.), http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm.

[41] OECD, "OECD Programme for International Student Assessment (PISA)," (n.d.), http://www.oecd.org/pisa/.

[42] Ibid.

critical infrastructure. The significant number of examples and case studies in social media will assist with analyzing the principles that drive information-sharing success. The literature does provide a descriptive view of areas to improve information sharing, which will be helpful when exploring if new principles can be applied to close those gaps. The research indicates opportunities for exploring examples of technical and operational applications of social media, extracting analysis principles of effectiveness and applying them against the shortcomings, and areas for improvement in the current state of information sharing for critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OVERVIEW OF THE CRITICAL INFRASTRUCTURE INFORMATION SHARING ENVIRONMENT

The CI ISE is the primary private sector component of the national information sharing environment. The environment itself is not a tangible system, network or program, but rather a collection of frameworks, policies, governance structures, and implementation systems that collectively contribute to the goal of sharing information between critical infrastructure stakeholders. It is widely considered that the large majority of infrastructure depended upon by the United States is owned and/or operated by the private sector.[43] The mission of protecting and ensuring resilience for the most critical of these infrastructures is largely a voluntary mission. The DHS is charged with leading this mission but must succeed with participation from both public and private stakeholders of the critical infrastructure community. In addition to federal agency colleagues who have related responsibilities for particular industries, the critical infrastructure community includes owners and operators, law enforcement and security professionals, industry association and security organizations, emergency managers, and planners and architects. Each of these stakeholder sets spans both the public and private sector and all levels of government. These facets, coupled together, make sharing information among stakeholders one of the most critical aspects of achieving a protected, secure, and resilient national infrastructure status. Information on threats, vulnerabilities, protective measures, best practices, trends, and much more, informs all parties and provides the value proposition for a call to action. Without the free flow of information, the stakeholder community has little to promote a necessity for measures or action.

For these reasons, the CI ISE is a fundamental component of critical infrastructure protection, and as such, is required to be efficient and effective at sharing information.

---

[43] U.S. Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors Characteristics : Report to Congressional Requesters* (2006), 63; The White House, "Sharing Information with the Private Sector," (n.d.), http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html; ISE.Gov, "Information Sharing Partnerships with the Private Sector—Owners of 85% of the Critical Infrastructure in the US," (n.d.), http://www.ise.gov/mission-partner/critical-infrastructure-and-key-resources.

A. CI ISE FRAMEWORK

The CI ISE is a framework, comprised of various components and facets, designed to provide a flexible and adaptable set of mechanisms by which the critical infrastructure stakeholder set can effectively share information. The CI ISE framework is intended to connect trusted and vetted communities of the public and private sector to collaborate over information exchange and collectively coordinate efforts toward the shared mission of the critical infrastructure protection. According to the 2012 Critical Infrastructure Information Sharing Environment paper (government distribution only), the framework is centered on a requirements-driven approach to information sharing.

The framework is described as meeting the core requirement of the Critical Infrastructure (CI) mission with three levels of decision making and action. These include strategic planning and investments, preparedness and situational awareness, and the execution thereof, and operational response and recovery. Within these decision categories, information varies in type. Table 1 describes the information types associated with each decision category.

Table 1. CI ISE Information Types by Decision Category

Decision Category	**Types of Information**	**Action**
Strategic planning and investment	Threat trends Criticality (consequence) Vulnerabilities Strategic solutions	Long-term protection programs Resilience planning and investments
Situational awareness & preparedness execution	Alerts and warnings Effective practices Training and education	Short-term protection and resilience actions Preparedness execution actions
Operational response & recovery coordination	Immediate threat notification Status reporting Requests for actions / information Common operating picture	Response actions Consequence mitigation Recovery actions Response and recovery coordination

The CI ISE is also grounded in several key principles to ensure alliance with the CI mission objectives and goals outlined in the QHSR, Presidential Policy Directives, and the NIPP. First, information must support the diversity of the stakeholder set, including the differing sectors, as well as the variances in operations and tempo for action. Next, information and information sharing are not ends unto themselves; rather, information enables alerts, threats, and other catalysts for action, informs risk management cycles, support collaboration on plans, strategies, best practices, and protective measures, and supports response and recovery missions.

The CI ISE is comprised of five essential elements that collectively address the requirements for the ISE, as outlined in the mission doctrine and guidance. These elements include the following.

- Governance Structure
- Relationship Management
- Delivery and Coordination
- Content Identification and Sourcing
- Information Safeguarding Programs

1. Governance Structure

As previously discussed, the CI ISE is inclusive of an expansive and diverse stakeholder set and is the framework and implementation facet of several national policies and directives. To balance this structure, the CI ISE employs a governance structure to collect and meet requirements systematically and consistently for information and the mechanisms to share it. The NIPP outlines a sector partnership as an organized structure among the CI community and stakeholders.[44] Within this sector partnership, councils have been established for each sector and both government and sector membership, and under the Critical Infrastructure Protection Advisory Council (CIPAC) mechanisms, are able to advise the government on critical infrastructure matters. The collective council set comes together as a cross-sector council to discuss and manage common goals and priorities of the community. Additionally, the NIPP describes

[44] Chertoff, *National Infrastructure Protection Plan*.

Information Sharing and Analysis Centers (ISACs) as operational components of many sector coordinating councils, as they support sector-specific information needs for threat/intelligence and vulnerabilities, and provide mechanisms for their memberships to collaborate on best practices, training, and education opportunities.[45] In some cases, ISACs have formal roles for the sector in incident response.

The CI ISE leverages these existing structures in the sector partnership to receive and validate requirements. The councils and ISACs represent, through sample membership, the larger CI ISE stakeholder set and can advise on both preferences for information-sharing mechanisms, but also requirements for content. This structure is also used in processes for the ISE membership and content delivery and use.

2. Relationship Management

In addition to the formal structures used in the governance structure element, the CI ISE relies on other relationships to ensure that information is available and disseminated to the greatest totality of the environment possible, which is important to ensure the objectives of the environment, and the CI mission that drive them, are met. Sector Specific Agencies (SSA) are those federal agencies assigned responsibility for the management of a critical infrastructure per Presidential Policy Directive-21.[46] They are responsible to work within their sector to implement the NIPP framework and to assess and mitigate the sector's risks. They serve as a main focal point between the federal government and the sector to coordinate infrastructure protection, incident response, and infrastructure recovery. Additionally, SSAs collect and disseminate information on their sector during emergency scenarios. Due to their expertise and relationships built with the owners and operators of the critical assets within their sector, they are a critical player in the CI ISE and can be leveraged to enrich content, dissemination practices, and contribute information and analytics.

The DHS Office of Infrastructure Protection (IP) forward deploys Protective Security Advisors (PSAs) across the country to work daily with owners and operators in

[45] Chertoff, *National Infrastructure Protection Plan*.

[46] The White House, "Presidential Policy Directive—Critical Infrastructure Security and Resilience."

local and regional settings. PSAs are a key liaison between federal agencies, state, local, tribal, and territorial governments, and the private sector, to develop and sustain trusted relationships in their area of responsibility. PSAs are uniquely positioned to have an understanding of the critical assets and infrastructures in their region and can deliver requirements from local stakeholders back to the DHS and the interagency, as well as facilitate the delivery of tools, training, and assistance to the owner and operator. PSAs typically have access to wider and broader stakeholder sets than may otherwise be captured through the formal council structures or direct interaction with a SSA, and consequently, they are an important extensive of the CI ISE.

3. Delivery and Coordination

Delivery and coordination represents the operational element of the CI ISE, in which information is shared via several mechanisms to and between stakeholders in the network. The National Infrastructure Coordination Center (NICC) is 24 hour, 7 day a week operations center responsible for monitoring, alerting, and maintaining situational awareness over the health and status of the nation's critical infrastructure. They maintain lists of partners contact information, organize stakeholder conference calls in incidents, develop situation reports for both federal and external partners, apprise DHS leadership of incidents and disruptions to critical infrastructure, and serve as a customer service" entry point for external partners with requests for information, reports of suspicious activity, and other inquiries for the department. The NICC relies on telephonic conferences, electronic mail, and the online secure but unclassified portal of the HSIN-CS to share information with partners.

ISACs serve as information dissemination and analysis hubs for some sectors within the CI ISE, which are typically operated by private sector organizations. The NIPP describes ISACs as being operational and tactical arms for sector information-sharing efforts and often provide information services during incidents.[47] ISACs are a force multiplier for the CI ISE and serve as a recipient of information from federal sources and

[47] Chertoff, *National Infrastructure Protection Plan*.

a disseminator of original content (including analysis) and information already in the CI ISE.

On both an as-needed and routine basis, the DHS and other federal, state, and local agencies may find need, purpose, or cause to share classified information with critical infrastructure stakeholders. Classified briefings are held in secure facilities and include invited participants of affected sectors to receive, and often discuss, classified information. In some cases, owners and operators of critical infrastructure are asked to consult on classified information products, which provide the government context for owner and operator mitigation and protective measures.

The CIPAC was established in 2006 by Federal Register Notice and establishes a forum and gathering body for discussing critical infrastructure policies, procedures, programs, and other related risk mitigation activities[48]. To ensure a robust partnership between government and private sector participants, and to enable voluntary collaboration and coordination, the CIPAC was created a Federal Advisory Committee Act-exempt body, which allowed for advice and consensus building to flow between partners without adherence to public disclosure.[49] On a regular basis, the DHS and other agencies meet with their counterparts via CIPAC and share information in the form of discussion, briefings, product delivery, and deliberation.

The HSIN-CS, in addition to being a primary mechanism for the NICC to share information, is the main technology platform of the CI ISE. It provides a secure online portal for the receiving and disseminating for information products, as well as information pieces (data, feeds, etc.). In mid-2013, the HSIN-CS platform migrated to the Microsoft SharePoint 2010 technology platform and is afforded the following capabilities.

- User-specified email alerts
- Web conferencing (Webinars)
- Document management

[48] Chertoff, *National Infrastructure Protection Plan*.

[49] U.S. Department of Homeland Security, "Critical Infrastructure Partnership Advisory Council," (n.d.), http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

- Real-time chat
- Discussion threads
- Incident and suspicious activity reporting
- Situational awareness
- Multiple levels of secure access
- Calendar tool
- Top-level publishing capability to share applicable DHS and other information resources with all sectors and regions simultaneously

The technology environment is structured as an upside down pyramid in which the greatest access is experienced by all users at the "top", and access becomes more tailored in sub-portals lower in the hierarchy. Sub-portals are designed with requirements and input from representatives of sectors or other mission organizations, and provide a tailored, and sometimes smaller, environment for particular users to collaborate and share documents with tighter controls.

4. Content Identification and Sourcing

Actionable information is cited as a continuing requirement from stakeholders of the CI ISE.[50] The framework of the CI ISE uses a "formalized process that identifies information and its source required to support community-specific communication, coordination, and collaboration procedures."[51] The requirements for content of this environment reflect on the source of information, where consideration is given to the validity or creditability of the information determined by the originating author or author organization. Additionally, the environment should consider the information overload phenomenon in which too much information can dilute the content and make any valuable content undiscoverable. To mitigate, the information-sharing environment includes functions for managing, organizing, and presenting information effectively. These functions allow the environment to adjust to the diverse stakeholder set that does not only span all different industries but also all levels of government (federal, state,

[50] U.S. Department of Homeland Security, *Critical Infrastructure Information Sharing Environment* (Washington, DC: U.S. Department of Homeland Security, 2012).

[51] Ibid.

local, tribal, and territorial) and all geographic regions across the country. Content management is a significant element in ensuring these stakeholder groups can find relevant information to meet their specific needs.

Content within the CI ISE is categorized as follows.

- Products—finished, published information pieces, such as situational reports, meeting records, threat bulletins, guides, fact sheets on critical infrastructure programs, etc.
- Tabular data—data or information pieces inputted through reporting tools, such as the suspicious activity reporting tool or the sector specific agency reporting tool. In these instances, users have the ability to complete forms for insertion into databases that can then be retrieved in tabular reports or spreadsheets.
- Information feeds—typically from open sources, information is presented in the CI ISE in feed format as inputted from other external sources. Feeds originate from media sources, as well as other information-sharing platforms within the CI ISE.
- Raw collaboration—while presently this type of information is not prevalent in online sources in the CI ISE, conversations, dialogue, and similar types of collaborations are prevalent in non-technical mechanisms, such as teleconferences, meetings, and briefings.
- Interactive media—the CI ISE provides training and awareness content to its stakeholders and is often delivered via electronic media and can include web-training, webinars, or virtual workshops hosted over collaboration media.

To ensure the CI ISE has relevant, actionable, and has timely information within itself, content providers are engaged in the content requirements processes to meet stakeholder group identified content specifications. Content providers are already included in the CI ISE to deliver their content directly to the stakeholder groups of the CI ISE in a single environment. Most often, content providers will provide information via the HSIN-CS either through direct post, through a sub-portal within the portal, or through the NICC. Content providers enrich the environment by pulling and placing content into a single mechanism already familiar to the receiving audience. In other words, by including content providers proactively into the CI ISE, stakeholders are disburden from many individually run portals and information sources, and can find and receive information from many sources in one place. With the aforementioned emphasis on content

management, information provided in the environment, regardless of its originating source or provider, can be presented, sorted, and filter according to many different content attributes.

5. Information Safeguarding Programs

The critical infrastructure protection, security, and resilience mission relies on the trusted partnership of infrastructure owners and operators. Information exchanged with owners and operators can be sensitive to that organization as it may reveal proprietary information about an organization, exposure security vulnerabilities, threats, and incidents to an organization and others. The CI ISE has several mechanisms to reduce the risk of sharing information beyond the critical infrastructure community or with organizations or individuals not poised or appropriate to receive it. While the CI ISE includes open-source, and otherwise unclassified information, it always includes sensitive but unclassified information, as well as classified information. Most commonly, the environment facilitates sharing For Official Use Only information, a term designated by the DHS to categorize sensitive information not otherwise categorized by statue or regulation.[52] The Protected Critical Infrastructure Information (PCII) program affords critical infrastructure information to be voluntarily submitted for explicit protection against from public disclosure, exemption from regulatory use, and assurance of appropriate safeguarding.[53] The program receives and evaluates information for protection under PCII, monitors and audits its appropriate handling and use, and provides certification for federal and state governments to receive, store, and use PCII appropriately.[54]

Presidential Executive Order 13549 directs the DHS to provide security clearances to private sector individuals to share sensitive and classified information

[52] U.S. Department of Homeland Security, *Critical Infrastructure Key Resources Information Sharing Environment White Paper*.

[53] U.S. Department of Homeland Security, "Protected Critical Infrastructure Information (PCII) Program," (n.d.), http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

[54] Ibid.

towards the goal of protecting their assets and infrastructure.[55] The private sector clearance program implements this direction and provides a nomination and determination of eligibility process for the issuance of security clearances to these stakeholders. Cleared private sector and government owners and operators are convened for periodic classified briefings that advise on the general risks and threats affecting the infrastructure community, threat-based briefings at which specific intelligence affecting one or many infrastructures is shared on an immediate need basis, and for return expertise from private sector experts who may advise on the potential impact or consequences of threats to infrastructure.

The CI ISE also considers protections for specially labeled and categorized information, which each associates with handling and release specifications. Information exchanged between the DHS and high-risk chemical facilities regarding vulnerability and security is labeled and protected as Chemical-terrorism Vulnerability Information, or CVI.[56] The Transportation Security Agency labels and protects Sensitive Security Information (SSI) for transportation-sector information sensitive for personal privacy, trade secrets, financial and confidential, or safety reasons, if the information was disclosed.[57]

B. CI ISE SHORTCOMINGS, CHALLENGES, AND GAPS

Despite the comprehensive framework and the diverse mechanism for sharing information, the CI ISE is reported to fall short of achieving its full potential, and thereby, diminishing the impact on the overall critical infrastructure mission. Criticism and recommendations for improvement center around the value of the information delivered within the environment, the totality of the stakeholder membership, and the nature of multi-directional collaboration between stakeholders. The following sections in

---

[55] *Executive Order 13549: Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities* (College Park, MD: Office of the Federal Register, National Archives and Records Administration, 2010).

[56] U.S. Department of Homeland Security, "Chemical-Terrorism Vulnerability Information," (n.d.), http://www.dhs.gov/chemical-terrorism-vulnerability-information.

[57] Transportation Security Administration, "Sensitive Security Information (SSI)," (n.d.), http://www.tsa.gov/stakeholders/sensitive-security-information-ssi.

this chapter review three studies each aimed at assessing the effectiveness of the CI ISE. These studies' findings follow and are categorically and summarized in a concluding table. These findings will be the basis for the areas in which the CI ISE may be improved by applying social media practices. Chapter VI presents this analysis.

1. Sources of Criticisms, Findings, and Areas for Improvement

The NIAC serves the President with advice on the security and resilience of the nation's critical infrastructure sectors and related information-sharing systems and activities. In 2012, the council completed a study and complimentary report aimed at determining the effectiveness of intelligence-information sharing within critical infrastructure. Specifically, the administration asked the NIAC to examine the progress and status of intelligence information sharing, as well as the sharing of counterintelligence, between the public and private sectors, and the role of fusion centers with respect to sharing intelligence with the private sector. The first two of these three objectives are most relevant to this thesis. While the CI ISE and critical infrastructure information sharing in general is aimed at sharing beyond just intelligence information, the NIAC's findings reveal several significant areas in which the environment could be improved.

The GAO has conducted several studies on critical infrastructure, and particularly, on information sharing with respect to security and protection. The June 2011 report entitled, *Rail Security, TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*, the GAO studied the Transportation Security Agency's (TSA) approach and execution of comprehensive risk assessments for the transportation sector.[58] (The transportation sector is one of the 16 critical infrastructure sectors outlined in Presidential Policy Directive-21. TSA is designated as the federal SSA for the transportation sector). The study found that while improvements had been made against previous recommendations, the rail industry, specifically, still seeks actionable information and analysis from the TSA. The report also outlines other opportunities for

[58] U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*.

streamlining information delivery. Prior, the GAO did a study with input from the American Public Transit Association (APTA) regarding the effectiveness the mechanisms by which information is delivered. The September 2010 report *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach* concluded that public transportation stakeholders had too many competing mechanisms by which to receive information.[59]

Along with the GAO reports, the following section summarizes the NIAC findings that directly related to delivery of and the collaboration on critical infrastructure information sharing, and omits findings centered on improvements within the intelligence community (IC) when developing content.

The NIAC concluded with five main areas of concern for intelligence information sharing. First, the NIAC found that the private sector does not receive the level of priority from the IC relative to its level of importance that it plays in the health of the United States and its economic security.[60]

Secondly, the private sector holds a vast and diverse knowledge base and an equally unique capabilities set.[61] However, the government, in many cases, does not understand these capabilities and knowledge, or in the cases in which it is understood, processes to leverage them are lacking. From its vantage point, the private sector can provide valuable context to address complex problems, adjudicate protective measures against a particular threat and vulnerability combination, and participate in risk mitigation solutions that will be effective for the greater critical infrastructure community. The private sector has the potential to contribute to the intelligence communities' counterterrorism efforts and is willing to share information bi-directionally to do so. The private sector perceives the government as ill prepared to receive, process, and understand its contributions for incorporation into intelligence products. Moreover, the NIAC found that intelligence information sharing mechanisms between the private sector

[59] U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

[60] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

[61] Ibid.

and the federal IC are redundant, confusing, and complicated, which makes the basic exchange of information a challenge for the critical infrastructure mission.[62]

Next, the NIAC found that incentives for sharing information between the public and private sector do not align with the critical infrastructure mission.[63] The private sector has adapted to a "need to share" approach to information sharing, while the public sector—particularly the federal IC, largely still operates on a "need to know" basis.

Fourth, federal intelligence information sharing is complex and confusing.[64] With 17 agencies in the federal IC, the private sector is challenged to navigate the complexities of each agency's role in collecting and disseminating intelligence. Meanwhile, agency diverse, yet similar, roles and missions makes mutual collaboration between the private sector and the IC prohibitive, and ultimately, encourages perpetuating personal relationships to share intelligence.

Finally, the NIAC charged that the DHS specifically is not championing adequately on the private sector's behalf within the IC.[65] The DHS's mission uniquely places the agency in a position to sensitize the IC to the critical infrastructure mission and the role the private sector plays in that mission.

2. Value of Content

Both the NIAC and GAO studies found a number of areas for improvement specific to this thesis including information content, information delivery, reach, and multi-directional collaboration. In addition to a general disposition that it does not receive the intelligence it needs, the private sector also finds most of the finished intelligence products it receives reactive to events rather than predictive.[66] The NIAC's study included the CI ISE and the HSIN-CS, the primary implementation technology for the CI ISE, and included interviews with over 200 stakeholders and extensive open-source

[62] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] Ibid.

research. The study revealed that stakeholders found the content of the CI ISE useful for static subjects, such as critical infrastructure protection background material and training on general CI topics, such as the NIPP and active shooter. Related, the study also found that users found content stale as it "does not provide real-time information limits its usefulness during fast-moving crises."[67]

Finished products are typically how information is packaged for dissemination to the private sector and the critical infrastructure community. However, fragmentary information is welcome, considered valuable, and important for receiving timely information. While the federal IC may not deem piecemeal information useful or digestible by the private sector, waiting for enough relevant information for a completed product is often too late for critical infrastructure to use in an actionable or timely way. Additionally, waiting for complete intelligence means missing an the opportunity for the critical infrastructure community to add relevant intelligence or provide context on what the intelligence information will mean for owners and operators, and how they may prepare or react to the information.

3. Information Delivery

Information delivery is generally thought to need improvement. The NIAC reported that intelligence-sharing processes, tools, and products are improving but significant progress is still required.[68] Most boldly, the NIAC asserts that the HSIN-CS, described in Chapter III is far from adequate for sharing intelligence information with the private sector and fall significantly short of the private sector requirements for an online information-sharing mechanism. HSIN-CS's technology platform does not support modern, off-the-shelf technology capabilities that would promote real-time analysis and sharing of intelligence. In addition to the substance of the content itself, a related challenge in today's information age is information overload. For the CI ISE, it means too much content is available to end users that results in frustration, and ultimately, a lack of the information needed due to the inability to find it. The NIAC found that its study

[67] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

[68] Ibid.

participants claimed "considerable time being spent to locate the needed information."[69] Similarly, the GAO found in their rail security study that the rail sector, a stakeholder group inclusive to the CI ISE, has multiple information platforms competing for stakeholder attention.[70] It should be noted that the three "competitors" identified in the study are recognized as part of the CI ISE.[71] The September 2010 GAO report on public transit security information sharing identified 12 different mechanisms for the rail industry to receive infrastructure security information and found that 69% of their survey respondents reported using at least five mechanisms collectively to receive information.[72]

4. Reach

Effectiveness of the CI ISE depends on information reaching the right people, as explained in the NIAC report.[73] An obvious extension is ensuring the CI ISE reaches not only the appropriate audiences but also the fullest extent of those audiences. Currently, the CI ISE participation is primarily measured by the HSIN-CS membership, which as of July 2012, was just over 15,000 users.[74] Considering the estimated thousands of critical infrastructure assets in the United States, the membership and inclusion in the CI ISE is far below the desired reach to deliver information to these partners effectively.[75] Membership criteria for the HSIN-CI are managed by the SSA of each sector, which may work with their sector coordinating councils, to establish the appropriate membership profile for potential users. Other membership criteria are established by DHS and outlines Federal, state, local government personnel access criteria. Outreach and advertisement for HSIN-CS is mostly communicated through PSAs and the SSA critical infrastructure

[69] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

[70] U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*.

[71] Ibid.

[72] U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

[73] National Infrastructure Advisory Council, *Intelligence Information Sharing*.

[74] U.S. Department of Homeland Security, *HSIN-CS Usage Statistics* (Washington, DC: U.S. Department of Homeland Security, 2012).

[75] John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report RL32631 (Washington, DC: Library of Congress, Congressional Research Service, October 1, 2004).

personnel. The NIAC report asserts that HSIN-CS has very limited exposure within the critical infrastructure sectors and believes the tool is very underutilized.[76]

The GAO study on public transit information sharing revealed that almost half of the industry agencies surveyed and studied did not have access to one of the main information sharing mechanisms (HSIN-CS or Public Transportation Information Sharing and Analysis Center (PT-ISAC)) and almost the same amount was not aware of those mechanisms existence.[77] Similar results were found in GAO report on rail transportation information sharing, where three information-sharing mechanisms were cited as delivering similar or the same information products to the same stakeholder set.[78]

5. Multi-Directional Collaboration

Multi-directional collaboration in the CI ISE is achieved when stakeholders interact as consumers and contributors to the environment, ideally on the same content. An example could be a discussion on a released information product or a request for information sent by a non-DHS stakeholder and responded to by a DHS stakeholder. A common criticism of the CI ISE is that information is uni-directional, and worse yet, information is commonly a pull from its primary mechanism, the HSIN-CS, which is true, however, across all the mechanisms by which information is shared in the CI ISE. As previously described, PSAs deliver information to stakeholders in the region. While doing so and over periods of time, the PSAs also collect information from the same partners, often in the form of asset data or security posture of infrastructure in their area.[79] While it may appear to be bi-directional information sharing, the information sharing is not on the same content and does not achieve true collaboration.

The September 2010 GAO report on Public Transit Security Information Sharing provided a description of the function of the PT-ISAC, which was mentioned earlier as a

---

[76] National Infrastructure Advisory Council, *Intelligence Information Sharing*, L-4.

[77] U.S. Government Accountability Office, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*.

[78] U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

[79] U.S. Department of Homeland Security, *Critical Infrastructure Information Sharing Environment*.

mechanism for sharing within the CI ISE. The GAO describes the PT-ISAC's functions as "collects, analyzes, and distributes security and threat information" and "disseminates this information through daily e-mails." The function description does not mention receiving information from stakeholders; rather, only from the federal government and open source. In this manner, the PT-ISAC as a CI ISE mechanism is not serving as an opportunity for collaboration and is reinforcing the complaint that information is uni-directional.[80] Further, the same GAO report identified 12 information-sharing mechanisms for the public transit sector, and of those, only one, the PT-ISAC, was identified to "push" information to end users.

The CI ISE does have some examples stating that this collaboration has been achieved. The HSIN-CS offers technology features to enable collaboration, and as in the case of the Northern California Regional Intelligence Center case study,[81] situations arise in which information is not only shared back and forth between stakeholders but the information sharing progresses over time as information is shared. In other words, as a situation unfolds, the information passed between parties progresses the topic, and ultimately, achieves a level of flow that adds value—be it situational awareness or operational intelligence.

[80] It should be noted, however, that the PT-ISAC and similar mechanisms are advantaged in the CI ISE to push information to stakeholders, rather than require a pull. While collaboration is still not provided, it does address the NIAC study's findings that information has to be pulled from the HSIN-CS. U.S. Government Accountability Office, *Public Transit Security Information Sharing, DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, 57.

[81] The Northern California Regional Intelligence Center (NCRIC) was the first fusion center to adopt the CI ISE by using the same framework of governance and policy, content, process, and technology to build a local information-sharing environment in the Bay Area. By following guidance and with assistance from the DHS Security Office of Infrastructure Protection, the NCRIC established an information sharing working group (ISWG) comprised of public and private sector partners in the region. Collectively, the ISWG established governance guidelines, procedures for sharing information, and delivered technical requirements to the DHS for the establishment of a tailored HSIN-CS sub-portal to execute the ISE functions. The northern California region exercised its CI ISE during the trial of a Bay Area Rapid Transit police officer in 2010. The trial was expected to, and subsequently did, cause civil unrest in the Oakland area. The CI ISE protocols were followed and information unfolded from both public and private partners of the region. As the incident unfolded over several days, contributions to discussion threads revealed action being taken by private sector business, the status of critical infrastructure (particularly transit), and information needs of the community. The environment also afforded an opportunity for the fusion center to share situation and incident reports as they were produced. National Infrastructure Advisory Council, *Intelligence Information Sharing*.

Table 2 summarizes the findings from the GAO and the NIAC studies as well as their cited gaps in the environment.

Table 2. Summary of CI ISE Gaps and Findings

CI ISE Gap Category	Specific Findings
Value of Content	A. Finished intelligence products are reactive rather than predictive. B. Information is packaged in products in lieu of sharing fragmented information, which is valuable and desired. C. Lack of input and context from the critical infrastructure stakeholders in information products.
Information Delivery	A. HSIN-CS is inadequate for sharing information with critical infrastructure stakeholders. B. HSIN-CS technology is out-of-date and generally not leveraging modern technology capabilities. C. Information overload, resulting in content discovery delays. D. Multiple delivery mechanisms are duplicative and confusing to the end user.
Reach	A. HSIN-CS has limited exposure to critical infrastructure stakeholders. B. HSIN-CS is underutilized.
Multi-Directional Collaboration	A. Information is uni-directional. B. Information is “pulled” from HSIN-CS. C. Information is typically only sourced from government sources.

IV. SOCIAL MEDIA OVERVIEW

Web 2.0 technologies are no longer a buzzword or new topic of discussion. Rather, these technologies are embedded in the day-to-day operations throughout the world, among all generations and walks of life. No longer a subject just for young technology enthusiasts, today, many interact with Web 2.0 technologies, or social media as it is often referred to, on a daily and even hourly basis. Facebook is a notable example of this type of information-sharing technology, and to date, has over 955 million users worldwide.[82] Twitter, a close rival for most-used technology of this kind, hosts over two million tweets a day.[83] The impact on the manner in which information is shared through many aspects of modern life is undisputable. Businesses have changed their models and leveraged this technology to market to new customers, provide competitive services, and appeal to modern requirements for information. In the context of homeland security, however, the pace to embrace this same exploding phenomenon is not noticeably as swift. Governments across all levels battle the advantages of using social media with the challenges and risk the same technologies present.

A. SOCIAL MEDIA DEFINED

Web 2.0 technologies refer to the second generation of the World Wide Web, in which paradigms for online information delivery shifted to capabilities and user experiences that offer user participation and promote collaboration through user-generated content.[84] Tim O'Reilly popularized the term Web 2.0 at the inaugural Web 2.0 conference in 2004.[85] Web 2.0 is used to describe a new utilization of the World Wide Web by technology developers, whereby content and applications were published through collaboration and participations of all users. Content was no longer restricted to one-way publishing by individuals or institutions. Web 1.0, by contrast, refers to an era of

[82] Facebook Newsroom, "Key Facts."

[83] Twitter Stats, "Popular Apps and Tweets."

[84] *Wikipedia*, s.v. "Web 2.0."

[85] O'Reilly, "What Is Web 2.0."

Internet browsing fueled by publishing, personal websites, static content, and directories.[86] While Web 2.0 does not refer to an actual technology update to the World Wide Web itself, it relies on basic functionalities to achieve a platform that allows for collaboration and dynamic participation.[87]

User Created Content (UCC) refers to the content publically available and created by end users. The OECD defines UCC as content having three requirements: 1) it must be published either on a publically available and accessible website or a social networking site accessible by select people, 2) it must demonstrate a creative effort, and 3) it is not created from professional routines or practices and free from remuneration and profit.[88] This definition excludes content exchanged in forums like email and private messaging, direct copy from existing sources, and content motivated by the commercial market.

Web 2.0 is a foundation platform for social media to thrive upon, while UCC is the summation of how people use social media.[89] Put another way, social media is a collection of capabilities and technologies, inspired by Web 2.0, that make it possible for a network of UCC. Notable and popular examples of social media tools include social networking sites, such as Facebook and Twitter, video sharing, such as YouTube and Vimeo, picture sharing (Shutterfly, Piascso), combination network and media sites, such as Instagram, collaboration projects like *Wikipedia*, and virtual gaming and social words, such as World of Warcraft and Second Life. It is important to distinguish that each of these examples represents tools that employ the concepts and principles of social media, and are not in themselves, social media. Kaplan and Haenlein categorize social media into six categories: 1) collaborative projects, 2) blogs and microblogs, 3) content communities, 4) social network sites, 5) virtual game worlds, and 6) virtual social

---

[86] O'Reilly, "What Is Web 2.0."

[87] Kaplan and Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," 61.

[88] Graham Vickery and Sacha Wunsch-Vincent, *Participative Web and User-Created Content: Web 2.0 Wikis and Social Networking* (Paris, France: Organization for Economic Cooperation and Development (OECD), 2007).

[89] Kaplan and Haenlein, *Users of the World, Unite! the Challenges and Opportunities of Social Media*, 61.

words.[90] Each of these categories embraces the two pillars of social media—Web 2.0 and UCC—but also embodies a set of principles and characteristics in which tools in these categories find success.

B. COLLABORATIVE PROJECTS

The purest manifestation of UUC, collaborative projects, seeks to bring users together to generate content dynamically and collectively. In theory, collaborative projects allow for a better outcome with group input and effort than from any one individual alone.[91]

1. Principle: Dynamic Content Editing

Dynamic content editing is a capability that affords the users the ability to create, edit, delete, cite, or report content directly into an online information-sharing environment. *Wikipedia* is a notable example of dynamic content editing in which any user can delete, edit or create content within an article. The word Wiki comes from the Hawaiian word "quick" and is a technology that allows users to edit content of a website easily, on their own, and quickly.[92] Adapted from the free online encyclopedia Nupedia, *Wikipedia* uses wikis to provide an online resource ever expanding to provide free information in 285 languages. The dynamic content editing principle applied to *Wikipedia* operates with a cost-free contribution model, where content is produced without pay to an organization or author.[93] The open system concept that *Wikipedia* (and its associated spawn—Wikitionary, Wikibooks, and Wikinews) employs breeds for honest reliable contribution. In 2005, *Nature* studied and compared 42 entries between Encyclopedia Britannica and *Wikipedia* and found only minor differences in accuracy between the two publications.[94] Brafman and Beckstrom assert that people in an open

---

[90] Kaplan and Haenlein, *Users of the World, Unite! the Challenges and Opportunities of Social Media*, 61.

[91] Ibid.

[92] Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 73.

[93] *Wikipedia*, s.v. "About."

[94] Giles, "Internet Encyclopaedias Go Head to Head," 900.

system will automatically want to contribute and they will do so with pride for accuracy.[95] While studying the effectiveness of *Wikipedia*, these authors also found that the majority of user created and edited content is positive. In the rare cases in which inaccurate or defacing content was contributed, it was corrected or removed by another user within hours.[96]

2. Principle: Group-Based Collection

Users collectively finding and sharing links to web articles or other content is considered group-based collection. Other users can rate the links or comment on the associated web content the link directs to, and thus, build a collection of user opinions across the web. Social bookmarking is a specific form of group-based collection in which bookmarking services do not store or save the resources themselves, such as photos or files.[97] Rather, bookmarks link to other content on the web. Users can add metadata to enable categorization, searching, and sorting of content. Other common features include a vote system to contribute a popularity or approval weighting to content, which is often used as a discriminator for display the content in a particular order or with an average positive or negative label.

With social bookmarking, an individual user will mark and label content personally, which is available to the user as bookmarks. Typically, an opportunity arises to share these bookmarks publically, or alternatively, content may be kept within a network of known fellow users.[98] Coalescing and aggregating many individual bookmarking lists creates a rich, robust catalog for an entire network.[99] The more tagged and weighted content, the richer the aggregation for a user discovering content through a social bookmarking capability. Social bookmarking tools also share this characteristic,

---

[95] Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, 74.

[96] Ibid.

[97] *Wikipedia*, s.v. "Social Bookmarking."

[98] Ibid.

[99] Hammond et al., "Social Bookmarking Tools (I) a General Review."

the more they are used, the more value accrues to the system itself, and thereby, to all who participate in it.[100]

Social bookmarking directly addresses the overwhelming nature of endless web content for any one individual to keep track of. Like a personal record of research sources organized by topic or research category, social bookmarking provides an organization system for individuals to monitor their interests across the World Wide Web. It also serves as a discovery tool for more content that may be of interest to a user. By displaying links by tags or allowing for sort by popularity, users are able to easily find and connect to information of interest.

3. Principle: Tagging

Labeling content by keywords and indexes has been a traditional organization on the web, but done so typically by an authority, such as a librarian or webmaster. Collaborative tagging provides a similar capability but allows for anyone to attach keywords and tags to content freely.[101] Collaborative tagging works in environments in which too much content is available for a single authority to manage and organize or in the absence of a librarian. Both these circumstances apply to the general web. Tagging allows users to personally choose how to label an item of content and also create a browsing mechanism to discover content created by others. Tagging is a main component of social bookmarking but is prevalent in many other types of social media categories, such as blogs and social networking sites.

Del.icio.us, or Delicious, is a common example of a social bookmarking tool that capitalizes on tagging to bring organization and management to content for its users.[102] Delicious provides online storage for an individual's personal bookmarks. Unlike bookmarking in a browser, Delicious affords users access to their bookmarks from any computer and browser, ideal for users who move between computers at work, home, and school. With an account, a user can bookmark webpages with the URL, title, and time of

[100] Hammond et al., "Social Bookmarking Tools (I) a General Review."

[101] Golder and Huberman, "Usage Patterns of Collaborative Tagging Systems," 1.

[102] Delicious, "About Us."

bookmarking saved. The users may tag the bookmark with one or many keywords of their choice. Users can see their bookmarks on their personal page listed in reverse chronological order. The personal page also has all the tags the users have given their bookmarks. Selecting a tag will display all the bookmarks with that tag attached. The social element of Delicious results from the networked community in which users can see the bookmarks that other users have collected. Delicious displays the most popular, or most bookmarked, URLs. User can also see any other user's personal page and filter by tag, much the same way they can view their own bookmarks. These features allow users to discover like content to a tag of interest or find other users with similar or common interests.

In social network sites, which are described in detail in a subsequent section of this chapter, tagging allows users, friends, and network acquaintances to follow conversations and discover content of interest. Value of content includes its applicability to the requirements and needs of the stakeholder, as well as the ability to locate and find the information appropriately. Twitter hashtags are examples of application of this principle. These tags allow contributors to classify the content they are authoring, while allowing consumers to subscribe to the same classifications and have content delivered to them. This principle is counter to traditional pull systems. The opportunity for users to self-subscribe to content of interest will vastly improve their ability to search and sort through the abundance on information.[103]

4. Principle: Crowdsourcing

Crowdsourcing refers to a large group of people corralled together to input into a common goal. The goal could be the creation of ideas, finding a solution to a problem, raising money, or authorship of content.[104] A key principle of crowdsourcing is to outsource the labor of the task at hand to a large network of contributors (or laborers) and with an open call for contribution.[105] The success of crowdsourcing—the result of a

[103] Kaplan and Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 59–68.

[104] *Wikipedia*, s.v. "Crowdsourcing."

[105] Crowdsourcing, "Crowdsourcing: A Definition."

crowdsourcing project to return a better idea, content piece, solution, etc. than would have otherwise resulted from traditional insourcing labor—can be attributed to the idea of crowd wisdom. James Surowiekci found that the collective wisdom of a group tends to aggregate greater than the wisdom of the smarter member of the group.[106] Applied to an online collection for group contribution, crowd wisdom allows for richer content or solution development. Crowdsourcing involves users—or the crowd—submitting solutions or contributions to the crowdsourcer. Sometimes, users who contribute to the ultimate solution are compensated in other cases; the pride of contribution serves as the reward. Crowdsourcing can solicit participation from amateur or general users or from professionals of a discipline related to the problem to be solved.

A notable example of competition-based crowdsourcing is the 2009 DARPA balloon experiment. To demonstrate the effectiveness of crowdsourcing against a geolocation problem, DARPA launched and moored 10 balloons at parks across the United States.[107] The competition called for the correct identification of all 10 locations and rewarded the first to do so a $40,000 prize.[108] The Massachusetts Institute of Technology Media Lab team found all 10 balloons in eight hours and 52 minutes days by recruiting over 5,400 individuals to contribute to finding the balloons. Chapter V explores the case study in more detail.

5. Principle: Crowdmapping

Ushahidi is an open source crowdsourcing collaboration platform for integrating multiple data feeds into an interactive map.[109] The principle Ushahidi employs is a variation of the crowdsourcing principle, in which the platform filters and displays with a dynamic timeline that allows the events to be tracked and mapped when and where they happened. Australia has embraced crowdsourcing over the last few years, and specifically, has employed Ushahidi to manage flooding and related issues in local

106 Surowiecki, *The Wisdom of Crowds*.

107 Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

108 Ibid.

109 Ushahidi, "Ushahidi."

communities. The Brisbane City Council combined social media capabilities by deploying a crowdsourcing map in January 2013 for citizens to report issues with flooding roadways by using a hashtag (#bccroads) or by filing out a report form on the website.[110] The data collected from hashtags and web forms were filtered and tracked on the Ushahidi map. The mapping software has an additional feature that confirms to the user if a report or issue has been verified, which eliminates concerns of inaccuracy or erroneous reporting by the public.

6. Principle: Voting

Content found in social media networks is often associated with a qualitative value. In some cases, it is reflected by how agreeable content may be, how often it is referenced or viewed, or a collection of positive or negative verdicts. The voting principle achieves a qualitative measure for content. The principle can be applied in various technological ways, but ultimately, seeks to achieve an opinion from viewers and consumers of the value of a particular content item. Facebook employs this principle with a "like" feature, where approving users can click their allegiance with a button. The count of total "likes" is shown under the content, and content with numerous "likes" is given preferential placement in newsfeed displays. On YouTube, a similar qualitative figure is given to a particular video by the number of views and ratings. In most cases, these values are used to promote and encourage additional viewership.

C. BLOGS AND MICROBLOGS

Blogs are the earliest form of social media and are categorized as typically being updated on a regular interval and displayed in reverse chronological order with a single author per blog post.[111] Blogs are most commonly in text form, but can include videos,

[110] Brisbane City Council, "Brisbane Storm and Flood Map," (n.d.), https://bnestorm.crowdmap.com/main).

[111] Vickery and Wunsch-Vincent, *Participative Web and User-Created Content: Web 2.0 Wikis and Social Networking*, 36.

photos, audio, or a combination thereof. The primary purpose of blogs is to share information, and sometimes, to receive information via comments or redirection to other sites or user created content.

1. Principle: Single Author Content

The main principle behind blogs is content is written and delivered from a single author.[112] Content is not generated collaboratively as with collaborative projects. Typically, a blog author is humanistic and personal, opposed to a company, brand or other organizational persona, and consequently, the tenor and tone of a blog is usually more personal than a traditional article or report on the web.

D. CONTENT COMMUNITIES

Content communities have the basic objective of sharing a media type between users. For examples, a community, such as YouTube, shares videos while Flickr exchanges photos among users.

1. Principle: No User Profiles

Often, content communities do not require a user profile to retrieve or share content.[113] Users are able to browse and post without creating a robust or in-depth profile. The lack of profile achieves easy, quick access to content without the burden of logins and maintaining accounts or profiles. The profile-less access also allows for anonymous consumption. Users are not necessarily tied to their content, or if they are, its personal history and bookmarking as opposed to an exposed profile, link their views to them.

E. SOCIAL NETWORKING SITES

Probably the most notable category of social media, social network sites are those sites that provide users with the opportunity to create personal online profiles, invite

---

[112] Kaplan and Haenlein, *Users of the World, Unite! the Challenges and Opportunities of Social Media*, 63.

[113] Ibid.

"friends" to share their content, and directly message and communicate within their network.[114] Profiles may include text, photos, videos, audio files and blogs that catalog interests, activities, and ideas. Wildly popular among all generations, these sites have become the principle mechanism many use to communicate. Notable examples of social networking sites include Facebook with 1.16 billion active users, and Google+ with over 500 million users.[115] Facebook is noted as the most popular web brand in the United States with 17% of consumer personal computer time spent on the social network site. As of 2012, 171.8 million people use social networking site in the United States.[116]

1. Principle: Personal User Profiles

Personal user profiles are the basic characteristic of social networking sites, and while many sites have very similar capabilities and features, each is unique. Profiles are typically generated based on a series of questions presented to the user upon registration to a site.[117] These questions include demographical information, such as age and location, as well as interests and more personal descriptors. Profile visibility varies from application to application. Facebook allows users within the same network to see each other's profiles by default, while other sites allow for public viewing of any profile, even by non-users.[118]

2. Principle: Choose Your Own Network

Motivation to use traditional social media, such as Facebook, Twitter, MySpace, etc., is reported to be connections within an individual's own networks, according to the Pew Research Center report, "Why Americans Use Social Media."[119] The easy

---

[114] Kaplan and Haenlein, *Users of the World, Unite! the Challenges and Opportunities of Social Media*, 63.

[115] Official Blog, "Google+: Communities and Photos"; Facebook Newsroom, "Key Facts."

[116] The Nielsen Company, "State of Media: The Social Media Report."

[117] Ellison, "Social Network Sites: Definition, History, and Scholarship," 210–230.

[118] Ibid.

[119] Aaron Smith, "Why Americans Use Social Media," *Pew Research Center*, November 15, 2011, http://www.pewinternet.Org/Reports/2011/Why-Americans-use-Social-Media.Aspx.

opportunity to stay in touch with friends, family, and co-workers drives participation in social media applications. Other reasons include connecting around a shared hobby or interest, or expanding an individual's network by meeting new friends.

The networked concept also assists in building multi-directional collaboration. Within an environment with user-defined networks that includes identity transparency, a significant opportunity for building trust emerges. Knowing who is in a network, where they work, their contributions to the environment, and other related details of their identity and connection to the network, encourages a more open and trusted environment to share. As Wayne Burke developed GovLuv, he was aiming "to build a system that would engender trust and respect between participants" and found this complexity of creating the culture of a network to be fundamental to that end.[120] Stakeholders' ability to choose their network, similar to "Friends" on Facebook, affords a level of assurance for the contributing user.

Networks are established by user identification and selection of users with whom they have a relationship. After joining a social network site, users are prompted to identify others in the system with whom they have a relationship. Displaying network connections is a significant factor of social networking sites, which enables users to move through connections of connections.[121] Discovery of potential new network first-degree connections, as well as new content, is thus possible.

3. Principle: Direct Communication

Direct communication affords users of social networking sites the ability to connect directly with other network users, which can be achieved through traditional "chat" features, in which two or more users can join an online chat conversation. Each user can immediately see each other user's entries and directly reply. Chat conversations are similar to text messaging on cell phones. Direct communication is also exemplified in posts on user profile pages, such as the Facebook "wall." In Facebook, users can tag other

[120] Wayne Moses Burke, "GovLuv," in *The Big Book of Social Media*, ed. Robert Fine (Tulsa, OK: Yorkshire Publishing, 2010).

[121] Ellison, "Social Network Sites: Definition, History, and Scholarship," 210–230.

users in their content posts, which make the content appear in those users' profile walls. Posts can also be directly placed on a user's own wall or directly on another wall. All these post examples comprise the news feed, on which any one user's compilation of a friend's activities and posts are listed chronologically. Similarly, Twitter uses direct communication. Any Tweet is discoverable by anyone in the Twitter universe, but using hashtags and user handles identifies a specific theme or Twitter user. These various mechanisms each afford a direct communication link between one or many users.

4. Principle: Casual Communication

The final principle of social networking sites is casual communication. Information is shared in disparate pieces, often short in length. Little to no restrictions exists on the content quality, such as completeness of sentences, or grammatical accuracy. In contrast to articles, publications, or reports, casual communication tends to be abbreviated and without circumstance or formality. In some cases, casual communication on social networking sites more closely resembles everyday verbal conversation. Content is not expected to be in complete form, either. Communication can occur in short strings of information rather than in completed format (like an article or report).

F. SOCIAL MEDIA PRINCIPLE SUMMARY

Table 3 summarizes the four social media categories and their associated principles. The table also references examples of social media applications that notably illustrate the application of the principle in their capabilities.

Table 3. Social Media Principle Summary

Principle	**Social Media Category**	**Description**	**Example Social Media Applications**
Dynamic Content Editing	Collaborative Projects	Directly create, edit, cite, or report content into an online environment.	*Wikipedia*
Group-based Collection	Collaborative Projects	Collectively finding and sharing links to web articles or other content.	Reddit Delicious
Tagging	Collaborative Projects	Freely attach keywords and tags to web content	Delicious
Crowdsourcing	Collaborative Projects	Large network of contributors input into a common goal, such as the creation of ideas, problem solutions, raising funding, or authorship of content.	Idea Scale
Crowdmapping	Collaborative Projects	Map with crowdsourced data that filters and displays with a dynamic timeline, allowing to events to be tracked and mapped when and where they happened.	Ushahidi
Voting	Collaborative Projects		Idea Scale Facebook
Single Author Content	Blogs and Microblogs	Content is written and delivered from a single author, typically in the form of a casually written article.	WordPress BlogSpot
No user profiles	Content Communities	Users browse and post without creating a robust or personal profile.	YouTube

Principle	**Social Media Category**	**Description**	**Example Social Media Applications**
Personal User Profiles	Social Networking Sites	Personal description and identity of a user.	Facebook MySpace
Choose your own network	Social Networking Sites	Users selected by a particular user based on a relationship or common interest.	Facebook Twitter
Direct Communication	Social Networking Sites		Facebook (direct message and wall posts) Twitter direct message
Casual Communication	Social Networking Sites		Twitter Facebook status updates

V. CASE STUDIES

A. CASE STUDY I: DARPA NETWORK CHALLENGE

In 2009, DARPA challenged the public with what came to be a significant exemplar of crowd sourcing and power of social media in a distributed challenge. The DARPA Network Challenge intended to demonstrate how a geo-diverse challenge could be solved by crowdsourcing.[122]

1. Background

The challenge awarded a $40,000 cash prize to the first team that could locate 10 red balloons located across the United States. The balloons were moored, 8-foot, and located in easily assessable locations seen from nearby roads. The locations were undisclosed and considered to be intractable by conventional intelligence methods.[123]

The contest occurred on December 5, 2009, and was announced on October 29, 2009, approximately one month prior to the challenge. DARPA had intended to launch the balloons daily, beginning at 10 a.m. Eastern time and concluding at 5 p.m. each day for a week until a winner was announced. However, the MIT Red Balloon Challenge Team won the competition in less than nine hours.[124]

DARPA estimates that at least 50 serious team competed seriously but as many as 100 participated in some capacity. Approximately 350,000 individuals are estimated to having a direct participatory role in the challenge, and some liberal estimates that counted mere knowledge of the challenge as it was happening as a participant, have total challenge participation at over 1 million.[125]

---

[122] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

[123] Ibid.

[124] CNN.Com, "MIT Wins $40,000 Prize in Nationwide Balloon-Hunt Contest."

[125] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

2. Case Study Deconstruction

DARPA Service Chief's Program (SCP) is comprised of military mid-career officers from all services on tour for three months with DARPA as fellows. As the DARPA Network Challenge was announced, the SCP monitored Internet traffic, media outlets, blogs, and team sites as they developed. They also convened scientists and researchers in social network analysis to inform them of a large-scale social network experiment that may be of interest for their own research and monitoring. Following the conclusion of the DARPA Network Challenge, the fellows interviewed 53 individuals who participated in the challenge and provided analysis and conclusions on a number of facets of the challenged, which are outlined in the *DARPA Network Challenge Project Report*.[126]

The DARPA SCP fellows identified 14 factors that affected the performance of any one team. Notable among the collection were several factors directly related to social media and social networks. Specifically, the fellows found a correlation between a team built around an existing social network or a social network associated with the challenge and the team's success. They also connected a team's ability to filter through Twitter posts for information relevant to the challenge. The fellows often found that eight tools contributed to a team's success for overcoming the geo-location diversity of the challenge. Typically, each team incorporated one or more of each of the tools. Among these tools, the teams employed a recursive, incentivized recruiting method among existing networks of friends and associates. Teams were able to extrapolate data regarding the location of balloons from open sources, such as Twitter, and an ability to do the data crawling automatically. Deployed technology, such as iPhone applications, was used to facilitate automatic reporting capabilities. Finally, websites designed to motivate and attract recruits while also providing secure reporting capability was another vital tool.

[126] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

The challenge teams drew upon three types of network hierarchies.

- Mass broadcast network hierarchy relies on large broadcasts to draw potential nodes into the network and notify them of the event. Optimizing search engine results and creative marketing techniques can amplify network growth in this hierarchy.
- The existing network hierarchy leverages pre-existing networks, which reduces all time required for constructing a network. While network construction is minimal, typically, existing network hierarchies still require time to mobilize for a particular event or task. In the case of the DARPA Network Challenge, teams leveraging existing networks were able to mobilize in less than 24 hours. This hierarchy was particularly useful in mobilizing geographically, a key component to the task of the challenge.
- Recruitment network hierarchy works on the principle that a chain of recruitment nodes will, in turn, recruit other nodes, which results in a potentially exponential growth curve. In the case of the DARPA Network challenge, most teams that employed this approached were able to incentivize each layer of recruited nodes by the game-like experience and the relatively low-cost in participating, which made it attractive for individuals to join teams and assist with the challenge and tasks of finding the balloons.

The MIT Media Lab Team—or the MIT Red Balloon Challenge Team—successfully located all 10 balloons in eight hours and 52 minutes. Notable, it was able to recruit over 5,400 individuals to participate in the challenge on its behalf in under 36 hours by using a recursive incentive recruiting method. The overall challenge promised an award of $40,000 to the winning team. The MIT team, citing a pure desire to use the challenge as a learning opportunity for its own research and studies, incentivized participation through promising to give all the money away to those who helped find the balloons.[127] Its website encouraged people to sign-up and assist the team and promoted that the first person to report the correct coordinates of each balloon would personally receive $2,000. To sweeten the incentive, the recruiter of the finder would receive $1,000, and the recruiter of the recruiter would receive $500. The incentive decreased each node of separation of the finder but allowed for multiple chances for any one person to receive a cash prize.

[127] CNN.Com, “MIT Wins $40,000 Prize in Nationwide Balloon-Hunt Contest.”

By contrast, the second place team—the Georgia Tech Research Institute (GTRI) I Spy a Red Balloon (ISARB) team—was one of the first to organize with almost the full four weeks to prepare. DARPA considered its site to be the best organized.[128] Leveraging its name recognition and positive and bountiful media coverage, the GTRI team employed the broadcast network hierarchy, and promoted its intention to donate the cash prize to charity.

George Hotz is one of the DARPA network challenge's most notable participant coming in a respectable third place. Hotz only learned about the challenge the day before it began and managed to locate eight balloons successfully with only an hour of preparation. Hotz, famed as a hacker, enlisted his 50,000 Twitter following to assist with the challenge. Hotz also incentivized his followers by promising a share of the prize ($1,000 to each finder) and a donation to charity.

The fourth place team, Groundspeak Geocachers, used its existing database of active geocachers to enlist in the cause. Geocachers were a fitting crowd to source because geocaching is an outdoor treasure hunt powered by GPS systems, which makes them naturally geographically diverse.[129] The database at Groundspeak was estimated to be the largest such collection of geocachers at the time of the DARPA Network Challenge, with a total data pool in the hundreds of thousands.[130] The Groundspeak team used the Geocacher database to solicit participation and notify followers via email alerts.

Other near-success teams employed the following strategies.

- Facebook friends' networks, with instructions for inviting an individual's own friends network to the cause.
- Brotherhood 2.0 vlog, a video blog leveraged to interest existing vlog followers with a viral video launched the day before the contest.
- Virtual operations center via Skype that allowed for real-time coordination of a misinformation campaign, targeted text messages, and report verification.

---

[128] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

[129] *Wikipedia*, s.v. "Geocaching," last modified November 19, 2013, http://en.wikipedia.org/wiki/Geocaching.

[130] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

- Close-knit, pre-existing networks centered around neighborhood watch organizations, which did not seek to expand the network but rather test the effectiveness of the existing capabilities of neighborhood watch networks. (This strategy found half the balloons).

The DARPA Network Challenge Project Report listed a number of observations from the contest.[131] First, based on the diverse network constructions with varying resources and commencement lead times, time to organize was not a factor in achieving the task. (Recall the winning team organized just two days before the contest). Next, mass media had a significant role in amplifying the networks, and in turn, the leading teams' successes. The predictability of traditional mass media coupled with the notoriety experienced by both leading teams led to quick reports of the 10 balloons with many watchful eyes. The report also cited Twitter as an extremely effective tool, with the capability of reaching thousands in minutes and receiving equally fast responses. The report did note, however, that Twitter is plagued with noise and enhanced filtering, and sorting and search methods, and algorithms are needed. Related, Facebook and using pre-established networks of friends proved effective as well. Perhaps most obviously, the DARPA Network Challenge validated that crowd sourcing is an effective mobilization mechanism for event detection. Using human sensors, the challenge demonstrated the power of corralling and coalescing small data points from many to reveal a clear and finite picture (the location of the 10 balloons).

The most notable observation from the DARPA Network Challenge Project Report is the simplicity of employing social networks to obtain high fidelity location and situational awareness extremely rapidly.

3. Social Media Principles and Outcomes

a. Crowdsourcing

Probably the most obvious application of a social media principle, crowdsourcing, was a key factor in achieving the DARPA challenge objective. The objective was challenged by geographic diversity and precise data required (the latitude and longitude coordinates of each balloon). In addition to finding all the balloon

[131] Defense Advanced Research Projects Agency, *DARPA Network Challenge Project Report*.

locations, competitors had to find the locations first to be victorious. Together, the challenge required real-time collaboration to compete effectively and find all the balloons. Each competitive team used the pooling of various resources to work together, collaborate, and ultimately, provide the necessary data to find the balloons.

b. Networks

To employ crowdsourcing strategies, the teams of the DARPA Network Challenge had to compile or leverage a network. These networks provided the "crowd" that was tapped as individual situational awareness resources, or means by which to include others that could, in turn, provide the data required to achieve locating each balloon. Networks employed varied, but typically included the "choose your own network" principle in which network nodes were already part of a network by choice. In these cases, individuals had either mutually decided to be "friends" with an existing participant of the contest (for those networks that leverage Facebook) or had chosen to "follow" a participant of the contest via Twitter or by subscribing to a network connected via email.

c. Direct Communication

In the cases of networks leveraged from social networking sites, such as Facebook and Twitter, the network served as a multiplier for each communication sent by the organizing team. Team messengers posted to Facebook, which in turn, is seen by all their "friends." One message tagged with each team member would have made the message seen by the summation of all the tagged friends' friends, although it is not evident if any of the teams using Facebook used this additional reach mechanism. Posts on Facebook would appear in news feeds, on which individuals can see a scrollable feed of recent updates from all their friends. Posts about the DARPA Network Challenge could be seen in the news feed or directly on any of the poster's personal wall. People viewing the post would have the opportunity to share the post on their wall, in turn, making it viewable by their entire friend network. Similar to the Facebook networks, those teams that used Twitter were able to reach all of their followers directly. With the ability to "retweet," Twitter users reaching the team's tweets could, in turn, share the

message with their followers. With both shares and retweets, receivers of the messages via an intermediary (their friend, friend of the poster) had the opportunity to join the root node, the team playing in the challenge. These shares and retweets, of course, grew the entire network, which made the crowdsourcing efforts all the more fruitful.

In addition to the teams being able to send messages to update their networks and appeal for their support in furthering their message, this principle means they were able to receive information quickly from their network. The crowdsourcing principle requires a network and a way for data to transfer between the root node and their network. By having direct communication capabilities through email, Facebook posts, Facebook direct messages, and Tweets, the players could receive sightings and data coordinates of located balloons. They could also verify the validity of reported sightings by receiving multiple reports at a time.

d. Voting

The teams using social media networking sites, such as Facebook, were able to perpetuate their messages further and penetrate them further with the "like" feature. The "like" feature allows a particular friend to demonstrate approval or general satisfaction with a post. The more "likes" a post receives, the more prevalent it is on news feeds. Friends of the "liker" will be notified their friend approved of a post—and what the post is—and in general, the post will receive higher priority on the walls of the poster's friends. Consequently, the reach for those communication pieces sent over networking sites with voting features was multiplied.

e. Tagging

Twitter users can follow conversations easily by finding and filtering Tweets with a hashtag of interest. In the case of the DARPA network challenge, teams using Twitter to enlist support and help labeled their Tweets with a known hashtag so their audience could follow the conversation. Likewise, teams looking for data from Twitter followers could filter in the same way. The tagging of conversations not only helps those interested in joining the conversation and following the game, it also cuts out

a lot of noise from the countless volume of tweets sent every minute. Hashtags were also an easy way for teams that employed misdirection and sabotage strategies to introduce false data into the conversation.

B. CASE STUDY II: DEPARTMENT OF STATE'S EDIPLOMACY

The DoS's Office of eDiplomacy aims to combine diplomacy with collaborative technology, which thus creates an innovated approach to knowledge sharing and supreme customer service.[132] The office was started in 2003 as a result of a recommendation to the DoS to improve its ability to communicate and share knowledge. Following the September 11, 2001, attacks, and the East Africa Bombings,[133] the DoS, under the direction of Secretary Colin Powel, began to shift from a culture of "need to know" to "need to share." Due to the nature of constantly rotating assignments by State officer personnel, the DoS is naturally challenged to manage, maintain, and organize institutional knowledge. At the same time, it is charged with ensuring officers on new duty assignments have the information necessary to meet the objectives of the assignments successfully, and in short order of onboarding. To meet these objectives, the office was created and uniquely combines innovative technology with diplomacy, and provides the DoS' employees with a variety of tools and resources to achieve these improved knowledge-sharing and communication goals. Many of the tools employed by the Office of eDiplomacy leverage social media principles. This case study highlights four of these tools and outlines how social media principles have contributed to the overarching information sharing goals of the eDiplomacy office.

1. Diplopedia

Bringing the same public collaboration experience to the internal networks of the DoS, Diplopedia is an online wiki for sharing information between DoS employees on

---

[132] U.S. Department of State, "IRM's Office of eDiplomacy."

[133] On August 7, 1998, a series of bombings at United States Embassies in the East Africa capitals of Dar es Salaam, Tanzania, and Nairobi, Kenya were carried out by the Egyptian Islamic Jihad. *Wikipedia*, s.v. "1998 United States Embassy Bombings," last modified November 27, 2013, http://en.wikipedia.org/wiki/1998_United_States_embassy_bombings.

its programs, offices, and international affair topics.[134] The online encyclopedia is classified as sensitive but unclassified. Diplopedia is available to DoS employees for direct collaboration and in read-only format to the U.S. government interagency. The resource is closed to the public. With registration, all DoS employees can read and edit content and are encouraged to do so.[135] Figure 1 is a screen capture of an example article on Diplopedia.

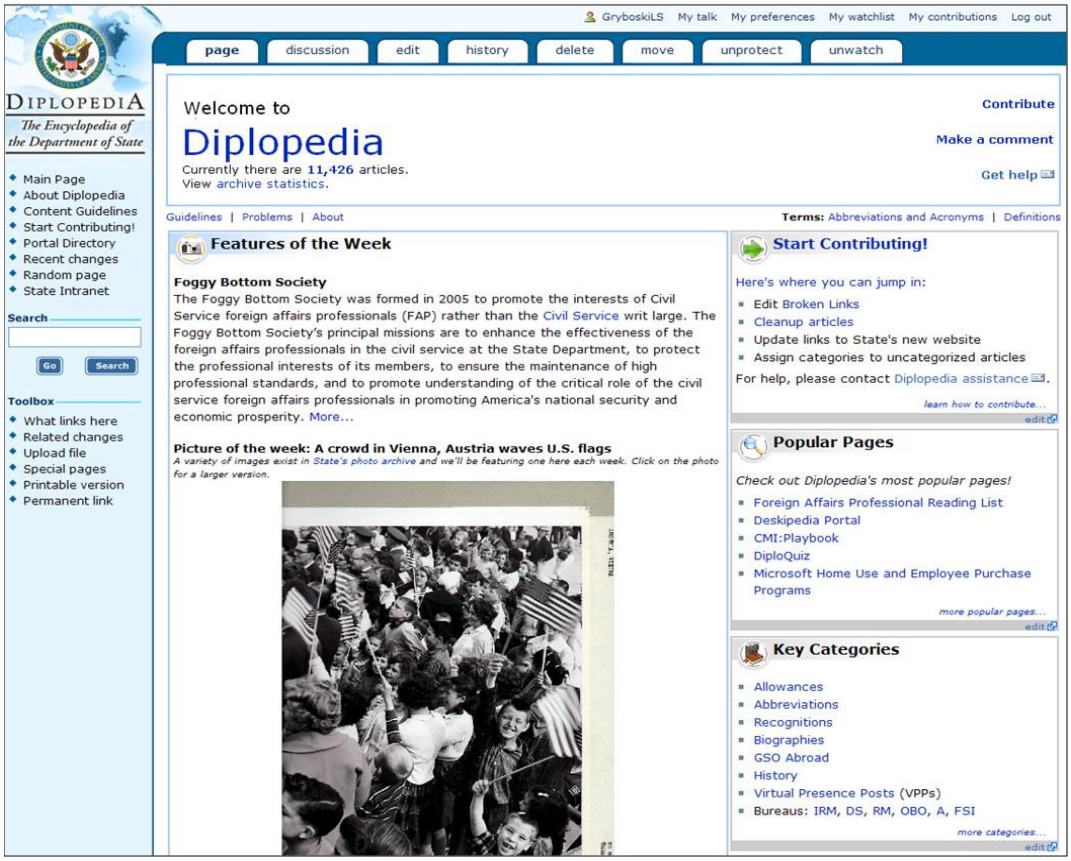

Figure 1. Diplopedia Screen Capture[136]

The Diplopedia governance guidelines cite ownership of the resource as belonging to all DoS personnel who contribute and use it.

---

134 *Wikipedia*, s.v. "Office of eDiplomacy," last modified November 20, 2013, http://en.wikipedia.org/wiki/Office_of_eDiplomacy.

135 U.S. Department of State, "About: Diplopedia."

136 Hanson, *Revolution@ State: The Spread of eDiplomacy*.

Unlike the well-known public wiki *Wikipedia*, Diplopedia does not allow anonymous contributions. All authorship must be done with registered accounts.

Disputes are purported to be infrequent but when they do arise, a panel of neutral and knowledgeable representatives is convened with a goal of maintaining a fair interpretation of opposing viewpoints.[137]

Diplopedia is considered a deliberative space, in which content is not considered final or necessarily endorsed by the U.S. government to allow for a collaboration space while products and other information pieces evolve towards completion. Articles can include links to finished resources to assist with the deliberative process. Fergus Hanson, after a four-month research embedment with the Office of eDiplomacy, found that one Washington, DC-based officer was tasked with reporting on religious engagement.[138] The report required input from posts around the world. To capture them, the officer created a Diplopedia page and asked that country reports be inputted directly to the report page. The final report on religious engagement was then created from the Diplopedia page. Diplopedia also includes a discussion tab feature, which is "behind" the article. Users can use the discussion tab to deliberate the substance of an article.

2. Communities @ State

In a similar spirit of encouraging collaboration within the DoS, Communities @ State ('Community') provides a forum for discussion and information sharing via blogs and blog communities. Communities @ State was born with the goal of establishing communities of practice around topics, process, or knowledge domains.[139] The blogs are designed to be easy to search, find, and encourage the experts in any domain to contribute to a topic in a horizontal information-sharing model (opposed to vertical stovepipes).[140] Unlike Diplopedia, community sites are typically open to the interagency foreign affairs

[137] U.S. Department of State, "About: Diplopedia."

[138] Hanson, *Revolution@ State: The Spread of eDiplomacy*.

[139] Bronk and Smith, "Diplopedia Imagined: Building State's Diplomacy Wiki," 593–602.

[140] Ibid.

community to transcend disciplinary and geospatial boundaries, and constraints.[141] The construct is a series of communities based on blogs written by the community members. The communities are self-forming and self-managed, and available on both classified and unclassified Intranet and interagency networks.

Community sites are comprised of administrators, readers, and authors. Authors can contribute content, but otherwise do not administer the site. Administrators are responsible for content and creating new topic areas within their community. They also have the responsibility for promoting and communicating about their community, as well as recruiting new participants. Administrators have the freedom to open their community to the interagency.

In addition to the community-structured blogs, personal blogs are also available for individuals to share experiences and individual perspectives on professional topics.[142]

3. Corridor

The Corridor is the DoS's internal online professional network.[143] Similar to LinkedIn—a public professional network, Corridor connects DoS personnel and other foreign affairs professional across the interagency. Participants maintain individual profiles, and are able to share professional accomplishments and interests. Like other online networking sites, users are able to choose and expand their networks through connections. The ability to search for other users by skill sets allows a transparent opportunity to expand networks. They can also join or create communities within their networks based on shared professional interests or experience. Leadership uses the formed groups to manage their teams and staffs, posting meeting minutes, action plans for upcoming goals, and collecting reports from staff on progress or their initiatives.

---

[141] U.S. Department of State, "IRM's Office of eDiplomacy."

[142] U.S. Department of State, "Major Programs of IRM's Office of eDiplomacy."

[143] Ibid.

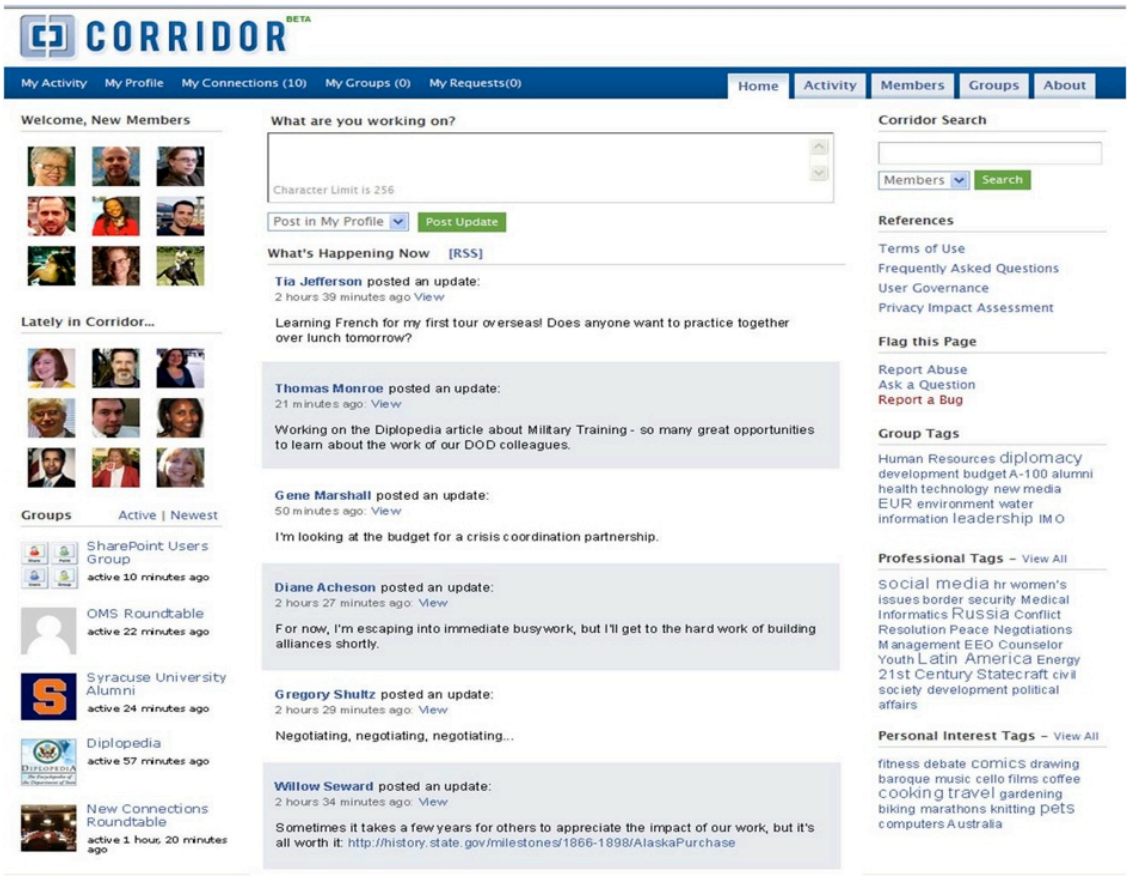

Figure 2. Corridor Screen Capture[144]

While Corridor possesses many similar attributes to familiar social networking sites (as shown in Figure 2), it varies in that all profiles are "public" to all DoS employees.[145] Users are not afforded the opportunity to hide messages or aspects of their profiles.

Corridor was deliberately designed to have the look and feel of Facebook so that users of Corridor would find familiarity and ease of use.[146]

The messaging and communication features of the Corridor promote an informal style of communication between staff, which results in quicker response time than with traditional, and more formal correspondence, such as email.[147]

---

144 Hanson, *Revolution@ State: The Spread of eDiplomacy*.

145 Ibid.

146 Ibid.

4. The Current

The Current is an information aggregator that affords DoS personnel the ability to pull information from internal and external websites into a single dashboard online. The personalized website imitates a personal briefing book or online newspaper completely customized by the individual. The main goal of the Current is to help professionals manage their information intake and prevent information overload from overwhelming the individual. An additional benefit, however, of the tool is the opportunity to deepen professional conversations through sharing information with users in the connected Corridor or Communities @ State platform.

5. Social Media Principles and Outcomes

a. Dynamic Content Editing

Employing the dynamic content editing principle, Diplopedia afforded its contributors and consumers the opportunity to directly author, edit, revise, cite, and discuss content directly in the environment. With basic guidelines, but largely relying on the community to maintain the integrity and appropriate guidelines of the platform, Diplopedia became a resource for foreign affairs specialists across the DoS, who are dispersed across many disciplines and geographical boundaries.

b. Single Author Content

Communities @ State took advantage of single author content with personal blogs collected around common themes and knowledge domains. Individual authors can write informational pieces on their experiences, expertise, areas of interest, or opinions. Consumers are able to read and process content from personal perspectives around common areas of interest.

c. Tagging

Tagging is used across the eDiplomacy suite, which allows consumers to follow subjects and topics through the various environments. Specifically, tagging is used

---

[147] Ibid.

in Communities @ State to ensure that blogs are collected and organized by topic, and in totality, searchable and sortable by keywords or topics. The Current uses tagging to organize information from many sources into one dashboard. Users can choose content based on tags and arrange content grouped in those tags into their own views.

d. Direct Communication

Direct communication is used throughout the eDiplomacy toolset. Diplopedia allows contributors to have "behind the scenes" discussions to debate and discuss content of a particular topic. In the Corridor, users with personal profiles can post content on their personal webpages (similar to walls in Facebook), as well as directly chat with other users.

e. Choose Your Own Network

The entire eDiplomacy platform encourages voluntary participation. Both the Communities @ State and the Corridor directly operate with users choosing their own networks. Coupled with the personal user profiles, the Corridor connects professionals virtually. These virtual connections promote opportunities for professionals to leverage their networks for knowledge transfer and professional assistance. Those using communities choose their own network but align to one or more community of blog conversation. Those within one community can author content around the groups' theme, consume other's comment, and comment on each other's content.

f. Personal User Profiles

Personal user profiles are created in the Corridor, which affords users personal profiles that can be populated with individualized content that distinguishes a particular professional based on experience and interests. The profiles are used throughout eDiplomacy to identify users as authors and contributors in Diplopedia and Communities @ State. The personal user profiles are also how users are able to connect with communities and networks, by reviewing profiles of interests.

g. Group-based Collection

Group-based collection is central to the Current as it pulls together content from many sources to display in one view or display. The Corridor also uses the group-based collection principle so that teams can use an area for teamwork, reports, meeting minute, tracking action plans, and other collaboration activities.

h. Casual Communication

The Corridor and Communities @ State both afford the opportunity for users to communicate casually. In the Corridor, coupled with direct communication, users can communicate and correspond through chat and message posts more quickly than through traditional communication. In Communities, users can share opinions and experiences without the formality of group-edited articles (like Diplopedia), which is an opportunity to share raw information.

C. CASE STUDY III: RIO DE JANEIRO EDUCATION REFORM

Since the mid-1990s, Brazil has experienced tremendous and impression growth in the quality and results in its education system. The rise of education in Brazil has been the fastest on record, second to China, and the country is considered a global leader in assessing student learning and education performance monitoring.[148] Nevertheless, despite the major improvement trends over the last 15 years, as recently as 2009, student proficiency in key subjects, such as math, is still averaging far below countries that are members of the OECD.[149] The OECD operates the Programme for International Student Assessment (PISA) study, which evaluates 15-year old student scholastic performance in math, science, and reading.[150] It was first conducted in 2000 and is repeated every three years. It is designed to assess the impact of education quality on income and for understanding achievement differences between nations.[151] The PISA test includes

[148] Bruns, Evans and Luque, *Achieving World-Class Education in Brazil: The Next Agenda*, 3.

[149] OECD presently has 34 member countries and was founded to stimulate economic progress and world trade. Education is a main policy area to which the organization contributes.

[150] OECD, "OECD Programme for International Student Assessment (PISA)."

[151] Ibid.

leveled questions in math. Level 1 questions are the lowest level of difficulty. In 2006, 80% of students from all nations taking the PISA test were able to answer the Level 1 math questions.[152] In Brazil, only 11% were able to pass these questions.[153]

Claudia Costin became the secretary of education for the municipality of Rio de Janeiro in 2008. She inherited an education system that while improving was still plagued as quite far from average scores and proficiencies of the OECD and like countries.[154] This case study explores how Costin employed a strategy to build trust with teachers, largely through the transparency of social media, to turn the education system around.

1. Challenges in Rio de Janeiro

At the time Claudia Costin took office as Secretary of Education, the one million students were testing 40% below grade level in math 28,000 students between fourth and sixth grades were completely illiterate.[155] Due to late starts, many students were years older than grade level and had to learn in classrooms with children two and three years younger. "Social promotion," in which students were passed to the next grade level regardless of achievement or preparedness, was a common practice.[156] The result of such an undereducated youth was girls preferring a profession in prostitution with a goal of having children by suitors ultimately to reach a more respectful status as mothers. Other children were exploited for narcotic trafficking.

The physical state of Rio schools was dismal, with buildings crumbling and basic utilities in complete disrepair. Long ago, the middle class had left Rio's schools, leaving only the desperately poor children behind. Civilian authorities had abandoned the areas of Rio controlled by drug traffickers; therefore, the schools were surrounded by gunfire and dangerous gangs. This danger had to be traversed every day by teachers and students

---

[152] Bruns, Evans and Luque, *Achieving World-Class Education in Brazil: The Next Agenda*, 27.

[153] Ibid.

[154] Ibid.

[155] Bratton and Tumin, *Collaborate Or Perish!: Reaching Across Boundaries in a Networked World*, 99.

[156] Ibid.

alike just to attend school. For these reasons, the teachers of Rio de Janeiro had long since felt abandoned. Their disenfranchisement resulted in chronic absenteeism.

Costin addressed these challenges by engaging the teachers and encouraging their participation in conversation and collaboration on improving the Rio de Janeiro education system. Costin knew she needed to engage the teachers with strong communication but she found the most effective tool by happenstance. Costin has five children who live all over the world. Wanting to connect with them via their generation's communication preferences, Costin started using Twitter to keep in touch.[157] The Tweets included an account of the initiatives Costin was employing in Rio, and to her surprise, the teachers of her municipality started following her.[158]

2. Twitter

Costin was not only surprised she had followers; she was curious what the teachers were interpreting in her conversations. Costin acted on her newfound tool. Since stumbling on the power of Twitter, she has committed to zealously using it to her advantage. She dedicates two hours each day to Tweet to her 16,000 followers. The Twitter conversations were a way to engage her teachers lightly in the collaboration process, and also provide consistent answers to her entire audience. It also served to make Costin extremely accessible, something important when reinvigorating a distant and tired employee base. In such an open environment, not all conversations are positive. While she was building trust, Costin faced offensive Tweets, but she responded positively, which slowly encouraged a trusted and positive online dialogue. This approach to the conversation allowed Costin to teach the teachers how to teach! She treated them as she hoped they would treat their students.

Twitter offered a direct link to Costin by bypassing bureaucratic chains of command. Costin had instant visibility on issues from building maintenance needs to serious incidents in a school. Costin was notified of malfunctioning bathrooms,

---

[157] Bratton and Tumin, *Collaborate Or Perish!: Reaching Across Boundaries in a Networked World*, 99.

[158] Ibid.

crumbling building structures, and the tragic uproar when an 11-year old child was shot to death during a drug gang crossfire.[159]

In addition to Costin's facilitated Twitter collaboration, the collaboration campaign also included email, a private online channel called "Fala, Professor!" ("Speak, Teacher!"), and an in-person engagement piece.[160] While Twitter was a light mode of collaboration, the "Fala, Professor!" platform served as a more serious space for online collaboration and work. Costin used the platform to begin the collaboration process with simple and straightforward questions. Costin challenged the online community to answer what the teachers should teach and what the students should learn. She cited the existing curriculum and asked for what should be changed. Couple with the conversations on Twitter and email, the "Fala, Professor!" platform accumulated a new standardized curriculum in just six months. Moreover, the curriculum had instant buy-in as it was co-produced, but also, thousands of the teachers would be empowered to deliver it.

3. Educopédia

With funding from the Ministry of Education, Costin asked 90 teachers to develop content to seed the new Educopédia—a Wiki-based platform for video, best practices, and digital classroom material.[161] Educopédia was shared throughout Brazil and today is a platform for both students and teachers. The platform includes "classrooms," which are reviewed by teachers of the Rio de Janeiro municipality, and includes lesson plans, guidelines, and activities that teachers can use in the classroom when teaching the corresponding curriculum.[162] In addition to teachers having the platform to share curriculum practices, students can access videos, games, animations, quizzes, and podcasts that help practice the lessons of each curriculum. Students can use Educopédia to keep pace with classes they may have missed, supplement their understanding of class

[159] Ibid.

[160] Bratton and Tumin, *Collaborate Or Perish!: Reaching Across Boundaries in a Networked World*, 99.

[161] Ibid.

[162] Educopédia, "Educopédia."

material, and generally to practice and improve their skills.[163] Figures 3, 4, and 5 are screen captures of English lessons available on Educopédia.

Figure 3. Educopédia Visitor Menu[164]

Figure 4. Educopédia Second Grade Student Menu[165]

[163] Ibid.

[164] Educopédia, "Educopédia."

[165] Ibid.

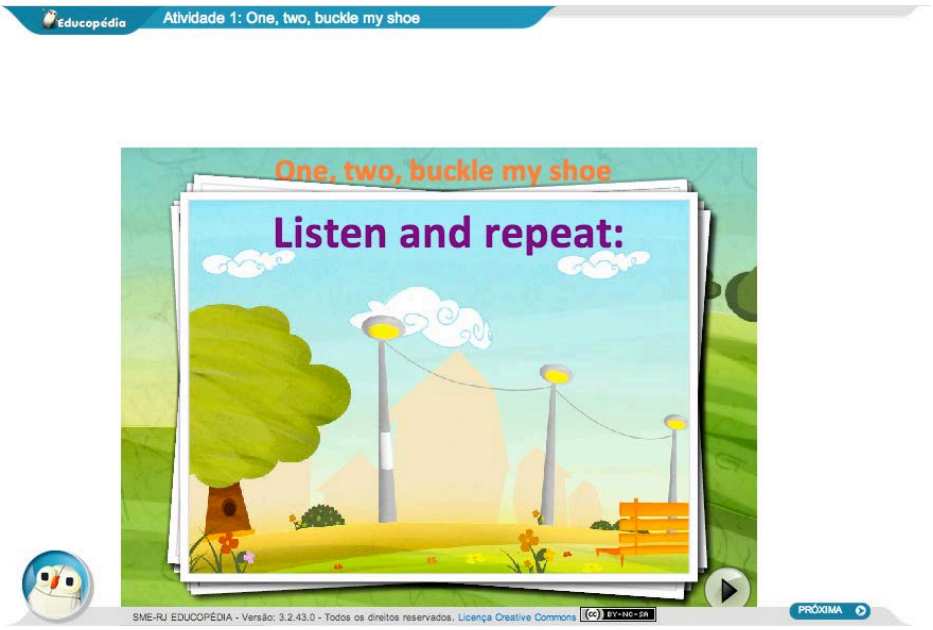

Figure 5. Educopédia Second Grade English Lesson[166]

The platform was specifically designed to be easy to use by both teachers and students, required no specific training, and was navigable by any level of computer literacy.[167] The platform requires a registered account and users login to access content. The stewards of Educopédia offer the platform to anyone via the visitor access feature.[168] Those who contribute at least 10 suggestions for improvement that are accepted are credited as "educopedistas."

4. Other Outcomes

Costin took her successes on social media platforms to the next level when addressing how best to use the curriculum to improve learning. She envisioned an education system that included laptops for every teacher to collaborate easily and uniformly connect. She also hoped for laptops for every three children and a projector in every classroom to emphasize the importance of the entire educational system to continue

[166] Educopédia, "Educopédia."

[167] Ibid.

[168] Ibid.

to remain connected and collaborating. A portal with blogs would allow teachers to share best practices, curriculum design, implementation techniques, and a strong platform for the teachers to assist each other.

5. Social Media Principles and Outcomes

a. Direct Communication

The launching success of Claudia Costin's revitalization of Rio de Janeiro's education system was directly engaging the teachers in the improvement process. Her use of Twitter and similar technologies enabled her to connect directly with over 16,000 teachers. She used direct communication to share information quickly and consistently with her audience. By continuing a responsive posture over direct communication, she quickly engaged in positive and productive conversations. Direct communication over Twitter was light and casual and allowed her to answers the questions of a few to the thousands of followers simultaneously, which ensured everyone had the same information. The direct access to someone that otherwise would be very inaccessible (likely most teachers would never otherwise converse or even meet the Secretary Costin), gave Costin a change to make significant (and small) changes with the information she was receiving direct, unfiltered.

Costin's "Fala, Professor!" also used direct communication, but this time, in a more private and intimate setting. The platform was used to probe teachers on specific subjects and projects Costin was working to improve. Teachers were able to directly input into conversations and share ideas in a closed environment.

The portal used among the Rio de Janeiro educators also allowed teachers to interact directly with each other. Blogs, chat, and other common features afforded these teachers the ability to engage one on one or in groups on items of interest or consume one teacher's perspective or experience from their point of view.

b. Choose Your Own Network

All the education improvement communication efforts Costin championed relied on the ability for users (teachers) to join at will and participate voluntarily. Costin's

Twitter network reached over 16,000 followers, which gave her an instant and direct platform to an enormous portion of her target audience. Even better, since each follower made the personal choice to join and follow, she had an open minded, ready-to-listen audience. The portal and "Fala, Professor!" also succeeded based on proactive participation by those who chose to join the conversation. The Educopédia system does not network users like Twitter, "Fala, Professor!," and the portal, but it also relies on active and willing participation. Educopédia also brings students and visitors into the platform, which thus expands the reach and use even further.

c. Group-Based Collection

Costin had the challenge of improving the fundamentals of the education system and that started with a modern, effective curriculum. Using group-based collection via "Fala, Professor!" gave her the opportunity to facilitate an online collaboration that piece by piece built a new curriculum based almost exclusively on the ideas and input of the teacher network engaged on the system. Perhaps unlike curriculum developed by administrators or education academics, this new curriculum had built-in buy in from the teachers, since they directly contributed to its development.

The Educopédia platform also exemplified group-based collection, which was populated exclusively with materials from its users. The platform houses lesson plans, best practices, classroom aids, and curriculum activities contributed by teachers. Organized by grade, subject, and specific curriculum item, the platform coalesced a diverse set of materials on any one lesson, a fruitful resource for any teacher, experienced or new. This platform also encourages suggestions and platform improvement ideas from its registered users. This form of group-based collection aids in the evolution of the system and ensures it continues to meet the needs of its constituents.

d. Dynamic-Content Editing

In addition to coalescing content from teachers and other contributors, Educopédia is based on dynamic-content editing to develop content on particular subjects with the input of many authors. Teachers, ensuring the content is up-to-date, valid and accurate, also review the "classrooms."

e. Single Author Content

Although most of the social media applications used to turn around the education system in Rio de Janeiro relied on group communication and collaboration, the portal still leveraged single author content. Via blogs, users (teachers) were given the chance to share their views in their own words and without edit.

D. CASE STUDY SUMMARY

The three studies presented above each used multiple principles of social media with varying outcomes. In all three studies, the outcomes ultimately improved the information-sharing component of the fundamental objective of the study subject. In turn, the objectives were met, for an overall success attributed to the application of social media. While the studies share the commonality of having used social media principles for the ultimate success of their objectives, they vary in the implementation of the tools. The DARPA case study exclusively leveraged available tools with social media principles. The DoS eDiplomacy built its tools in house. The Rio de Janeiro used existing tools like Twitter but also benefitted from tools built specifically to the needs of the education community. In all cases, however, social media principles were applied and responsible for information-sharing outcomes. Table 4 summarizes the principles each case study employed and the related information-sharing outcome that resulted from the use of the principle.

Table 4. Summary of Case Studies Principles

CS1: DARPA	Crowdsourcing	– Pooled resources to find the needed data collectively
	Networks	– Provided the "crowd" the crowdsourcing principle – Provided necessary geographic diversity – Instant participation by thousands from existing networks
	Direct Communication	– Messages penetrated deeply into network – Messages are directly viewed or view by happenstance in feeds – Promoted cause, encouraged viewers to join network – Mechanism to receive data directly the from network
	Voting	– Promoted content, strengthened the visibility
	Tagging	– Network could easily stay engaged in the conversation – Data was found and received in an organized manner – Focused the conversation to filter out noise
CS2: eDiplomacy	Dynamic Content Editing	– Provided resources for subject matter expertise and real professional experiences without overhead of publishing (professional authors, editors, etc.). – Allowed for information sharing between colleagues, separated by geographically diverse assignments – Captured knowledge of many experiences on a single subject into one source
	Single Author Content	– Provided perspective of an individual author's experience and opinions, with little to no filtering or editing
	Tagging	– Connected content across the eDiplomacy suite, integrated conversations on similar topics or themes in the blogs, personal profiles, articles,

		and content integrator
	Direct Communication	– Allowed users to discuss or debate content while in development, enriched the information ultimately published (creditability?) – Users could directly converse, faster than traditional communication, such as email.
	Choose Your Own Network	– Connected professionals virtually – Promoted opportunities for knowledge transfer and professional assistance within networks
	Personal User Profiles	– Identified authors and contributors for transparency and validity – Enabled network creation by browsing profiles, filtering on interests and experience
	Group-based Collection	– Organized content from within and outside of eDiplomacy, made content easy to read, found it, and archived it – Provided virtual workspace for teams to collaborate, share materials in a central, transparent location
	Casual Communication	– Encouraged communication by avoiding the formalities of traditional communications – Allowed for raw information sharing, including opinions and personal experiences
Rio de Janeiro	Direct Communication	– Provided accessibility to leadership from teachers, a direct link that would ordinarily not be possible without significant bureaucratic processes in between. – Allowed for quick response to information received – Consistent and broad messaging – Direct input into collaboration projects
	Choose Your Own Network	– Created completely voluntary network, willing to engage and work on improvements – Open minded, willing audience – Inclusive (teachers, public, administrators, students)

	Group-based Collection	– Quick development of new curriculum – Instant buy-in to new system – Expert and diverse content to aid others
	Dynamic-content Editing	– Content developed “for free” by teachers, as opposed to hired academics or administrators – Content enriched by perspective of many authors – Genuine content
	Single Author Content	– Personal views and experiences shared

VI. ANALYSIS

In the preceding chapter, each case study was reviewed for outcomes that resulted from the use of the social media principles defined in Chapter V. The objectives of the CI ISE were described in Chapter III, along with the shortcomings and criticisms reported against the environment. The combination of original objectives and documented failures are combined for a complete list of the ideal characteristics of the CI ISE. By comparing the desired characteristics of the CI ISE against the outcomes seen in the case studies, potential relationships of common successes desired by the CI ISE and achieved by the case study emerge. The following chapter details the data and its compilation to setup an analysis of case study outcome to CI ISE characteristics and potential social media principles that may be applied to the CI ISE to achieve similar outcomes.

A. THE DATA

Chapter III summarized the main objectives of the CI ISE and listed the commonly sourced shortcomings that keep the environment from fully supporting the information-sharing requirements of the voluntary critical infrastructure protection mission. These shortcomings were transfixed into additional characteristics the environment would need to include to reach the potential utility required for the mission and added to the original objectives. The characteristics organize into four categories: 1) value of content, 2) information delivery, 3) reach, and 4) multi-direction collaboration. The 21 characteristics and their associated categories are summarized in Table 5.

Table 5. CI ISE Characteristics

Value of Content
Finished intelligence products should be predictive (opposed to reactive).
In addition to static information, content should be fresh, up-to-date, and where possible, provided in real-time.
Content should be available in fragments (raw) or in finished, complete formats.
Context from owners, operators, and industry subject matter experts should be applied before products are finished.
Alerts, threats, and catalysts for action should be provided.
Content encourages action and participation.
Content is diverse, providing value to multiple facets of the CI ISE.
Content is relevant to the stakeholders of the CI ISE.
Information Delivery
Real-time delivery of content.
Organized content (easy to find, searchable, sortable, etc.).
Limited mechanisms across CI ISE to receive information.
Information flows freely through the environment, without barricade or burdensome process.
The environment should push information to stakeholders and allow for pull at anytime.
Reach
Content should reach appropriate audiences for accomplishing the critical infrastructure mission.
Content should reach fullest extent of appropriate audiences.
The environment should connect trusted and vetted communities.
The environment should include a diverse stakeholder set, representing the entire critical infrastructure mission.
Multi-Directional Collaboration
Stakeholders within the environment should participate as both consumers and contributors.
Content should be sourced from all stakeholder types.
The environment should allow for coordination of efforts on response and recovery missions.
The environment should allow for collaboration on plans, strategies, best practices, protective measures.

Chapter VI summarized the outcomes of each case study. These outcomes have been attributed to a social media principle based on the definitions and understanding of their utility as described in Chapter V. The case studies produced 40 outcomes mapped to 13 social media principles. Each outcome was linked to one principle. Over the three case studies, each principle was evident in many outcomes. Each outcome was labeled with an identifier to make correlation in the analysis easy to follow. The syntax is as follows:

DARPA Network Challenge → Case Study 1 → CS1:[Outcome X]
Department of State's eDiplomacy → Case Study 2 → CS2:[Outcome X]
Rio de Janeiro's Education Reform → Case Study 3 → CS3:[Outcome X]

Table 6 depicts the intersection of each outcome to a social media principle.

Table 6. Case Study Outcomes Mapped to Social Media Principles

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS1:1	Pooled resources to collectively find data needed				x								
CS1:2	Provide the "crowd" to for the crowdsourcing principle										x		
CS1:3	Provided necessary geographic diversity										x		
CS1:4	Instant participation by thousands from existing networks										x		
CS1:5	Messages penetrated deeply into network											x	
CS1:6	Messages are directly viewed or view by happenstance in feeds											x	
CS1:7	Promotes cause, encouraging viewers to join network											x	

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS1:8	Mechanism to directly receive data from network											x	
CS1:9	Promotes content, strengthening the visibility						x						
CS1:10	Network can easily stay engaged in the conversation.			x									
CS1:11	Data is found and received in an organized manner.			x									
CS1:12	Focus the conversation to filter out noise.			x									
CS2:1	Provided resource for subject matter expertise and real professional experiences without overhead of publishing (professional authors, editors, etc).	x											
CS2:2	Allowed for information sharing between colleagues, separated by geographically diverse assignments	x											

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS2:3	Captured knowledge of many experiences on a single subject into one source	x											
CS2:4	Provide perspective of an individual author's experience and opinions, with little to no filtering editing								x				
CS2:5	Connects content across the eDiplomacy suite, integrating conversations on similar topics at themes in the blogs, personal profiles, articles, and content integrator			x									
CS2:6	Allows users to discuss or debate content while in development, enriching the information ultimately published (creditability?)											x	
CS2:7	Users can direct converse, faster than traditional communication such as email.											x	

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS2:8	Connects professionals virtually										x		
CS2:9	Promotes opportunities for knowledge transfer and professional assistance within networks										x		
CS2:10	Identifies authors and contributors for transparency and validity									x			
CS2:11	Enables network creating by browsing profiles, filtering on interests and experience									x			
CS2:12	Organizes content from within and outside of eDiplomacy, making content easy to read, find, and archive.		x										
CS2:13	Provides virtual workspace for teams to collaborate, share materials in a central, transparent location		x										
CS2:14	Encourages communication by avoiding the formalities of traditional communications												x

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS2:15	Allows for raw information sharing, including opinions and personal experiences												x
CS3:1	Provided accessible to leadership, not likely otherwise to be achieved											x	
CS3:2	Allowed for quick response to information received											x	
CS3:3	Consistent and broad messaging											x	
CS3:4	Direct input into collaboration projects											x	
CS3:5	Created completely voluntary network, willing to engage and work on improvements										x		
CS3:6	Open minded, willing audience										x		
CS3:7	Inclusive (teachers, public, administrators, students)										x		
CS3:8	Quick development of new curriculum		x										
CS3:9	ınstant buy-in to new system		x										

ID	Outcome	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
CS3:10	Expert and diverse content to aid others		x										
CS3:11	Content developed “for free” by teachers, opposed to hired academics or administrators	x											
CS3:12	Content enriched by perspective of many authors	x											
CS3:13	Genuine content	x											
CS3:14	Personal views and experiences shared							x					

B. DATA COMPILATION

Each characteristic of the CI ISE was reviewed against the outcomes observed in the three case studies. Where outcomes seen in the case studies related to the characteristic of the CI ISE as a similar outcome expected with the characteristic, a match was recorded. For each CI ISE characteristic, many outcomes related and served as exemplars for the ISE. In turn, each of these outcomes associated with a characteristic has an associated social media principle. Thereby, each CI ISE characteristic can be related to the same social media principles as the mapped case study outcomes. The resulting mapping correlates desired characteristics with potential principles that may yield similar outcomes as the case studies.

Table 7 associates the CI ISE characteristics with the principles seen in the case study outcomes. For each case study outcome, the principle attributed to that outcome was cataloged next to the CI ISE characteristic. After mapping each characteristic to outcomes and then principles, each characteristic had at least two case study outcomes. It is evident that in many cases the same principle was prevalent in more than one outcome that related to a particular characteristic. For example, the CI ISE characteristic: content should reach appropriate audiences for accomplishing the critical infrastructure mission. The following case study outcomes were directly relevant.

- CS1:1—Pooled resources to find the needed data collectively
- CS1:3—Provided necessary geographic diversity
- CS1:7—Promotes cause, encourages viewers to join the network
- CS2:11—Enables network creation by browsing profiles, filtering on interests and experience
- CS3:3—Consistent and broad messaging
- CS3:5—Created completely voluntary network, willing to engage and work on improvements
- CS3:7—Inclusive (teachers, public, administrators, students)

These outcomes collectively are attributed to the social media principles of personal user profiles, choose your own network, and direct communication. Subsequently, this characteristic is mapped twice to personal user profile, four times to

choose your own network, and twice to direct communication. Table 7 reflects “2,” “4,” and “2” in the row for this characteristic in the respective principle columns.

Table 7. CI ISE Characteristic and Case Study Outcome Principles

	Social Media Principle											
	Dynamic Content Editing	**Group-based Collection**	**Tagging**	**Crowdsourcing**	**Crowdmapping**	**Voting**	**Single Author Content**	**No user profiles**	**Personal User Profiles**	**Choose your own network**	**Direct Communication**	**Casual Communication**
Value of Content												
Finished intelligence products should be predictive												
Content should be real-time				**1**						**1**	**2**	
Fragmentary information	**1**			**1**				**1**				**2**
O/O; industry context before products are finished	**2**	**3**		**1**			**1**	**1**			**2**	
Enable alerts, threats, catalysts for action										**1**	**3**	
Content encourages action and participation			**1**			**1**				**1**	**1**	**1**
Content is diverse	**2**	**1**										
Content is relevant	**2**	**1**										

	Social Media Principle											
	Dynamic Content Editing	**Group-based Collection**	**Tagging**	**Crowdsourcing**	**Crowdmapping**	**Voting**	**Single Author Content**	**No user profiles**	**Personal User Profiles**	**Choose your own network**	**Direct Communication**	**Casual Communication**
Information Delivery												
Real-time Analysis (technology capability)												
Organized Content (easy to find)	**1**	**1**	**3**									
Limited mechanisms or complete mechanisms to receive information	**1**	**1**	**2**								**2**	
Free-flow of Information	**1**						**1**				**3**	**1**
Reach												
Reach appropriate audiences									**2**	**4**	**2**	
Reach fullest extent of appropriate audiences			**1**							**2**	**2**	
Connect trusted and vetted communities	**2**								**2**	**4**	**2**	
Diverse stakeholder set	**1**						**1**		**1**	**3**		
Push											**4**	

	Social Media Principle											
	Dynamic Content Editing	Group-based Collection	Tagging	Crowdsourcing	Crowdmapping	Voting	Single Author Content	No user profiles	Personal User Profiles	Choose your own network	Direct Communication	Casual Communication
Multi-Directional Collaboration												
Stakeholder consumers and contributors	**3**		**1**					**1**	**1**	**1**	**3**	
Sourced from all stakeholders	**4**		**1**								**1**	**1**
Coordinate efforts on response and recovery missions		**1**	**1**	**1**						**1**	**1**	
Collaborate on plans, strategies, best practices, protective measures	**1**	**2**	**1**	**1**							**2**	

C. ANALYSIS

The case studies described in Chapter VI represent three distinct scenarios with the common objective of effectively achieving a unique goal by sharing information. Each case study achieves a measurable level of success against each study's goal. Specifically, the DARPA Network Challenge aimed to study crowdsourcing but had an even simpler goal of having a team or individual locate 10 geographically diverse balloons. The contest provided DARPA a sizeable amount of data to study related to crowdsourcing, as well as the various techniques and strategies employed by the competing teams. The simple goal of finding the balloons was swiftly met in less than nine hours. Both these goals were met with the assistance of social media principles.

The DoS aimed to provide an integrated enterprise environment that would enable knowledge sharing and management among their Foreign Service personnel. It achieved this goal with several platforms, each employing a series of social media principles applied with similar technology to that seen in public realms, but in a closed environment. The DoS achieved success in a closed environment and was able to integrate its multiple platforms to create an integrated environment.

Rio de Janeiro seized on the happenstance success of Secretary Costin's personal use of Twitter to amplify information-sharing efforts across public and private social information-sharing platforms. The objective—to improve the education system and facilitate reform—was met through several applications of social media principles. This case study demonstrated application using public and well-known information-sharing technologies, such as Twitter, as well as applying the social media principles in closed environments.

While these case studies do not represent a homeland security mission, they achieved similar outcomes as to what is desired by the CI ISE. By studying the outcomes experienced in each of the case studies, and correlating the social media principles responsible for those outcomes, potential matches for applying the principles to the CI

ISE emerge. The following sections depict each objective area of the CI ISE (covered in detail earlier in Chapter III), and the emergent principles from the corresponding case study outcomes.

1. Improving the Value of Content

The CI ISE has eight main characteristic objectives aimed at improving and ensuring the content in the environment is valuable to the stakeholders (see full list in Table 5). Content that can assist the community with its individual efforts towards protecting, securing, and making resilient infrastructure must be available both statically and in real-time, should include perspectives from both the public and private sector, and encourage continual participation in the mission. The following section outlines the findings of comparing the case study outcomes and their associated social media principles to the broad goal of improving the value of content in the CI ISE.

The CI ISE has a basic objective to ensure that information flows in all directions within the CI ISE. Related, the NIAC underscored the importance of leveraging industry expertise when compiling products or other content pieces. Reviewing the case studies, 10 outcomes align to this CI ISE characteristic of ensuring 360-degree contribution to content. Three of those outcomes suggest that group-based collection would assist with this objective and two outcomes tie dynamic content editing to achieving this sort of goal. Leveraging direct communication, crowdsourcing, single-author content, and no user profiles all are possible principles that when applied in the CI ISE, would also help achieve this goal. As seen in the Rio de Janeiro case study, group-based collection assisted in completely rewriting the education curriculum and had the added benefit of instant stakeholder buy-in, since they directly contributed to the development. This type of group collaboration would also meet the objective in the CI ISE of leveraging the expertise of industry when developing content on a best practices guide, a protective measures guide against a common vulnerability, or a threat product.

The CI ISE also strives to include more fragmented information to allow for expanded use of raw information by the stakeholders and to facilitate faster access to information. Comparing the outcomes of the case study, dynamic content editing,

crowdsourcing, and no user profiles, all will assist with facilitating raw information sharing. Two outcomes point to the casual communication principle to ensure fragmented information is available in the CI ISE. Four of the five outcomes across the case studies that applied to fragmented information came from the DoS's eDiplomacy case study. The Diplopedia allows individuals to contribute in a group environment with sporadic pieces of information, and does not require any one author to contribute a complete product. In the Corridor, users can communicate and correspond through chat and message posts more quickly than through traditional communication, and with less formality. The blogs in Communities @ State give any one author the chance to share information directly in any style and without a publishing process. Similar capabilities using the same casual communication principle in the CI ISE can be expected to produce a similar result, in which stakeholders have multiple opportunities to contribute directly in a less formal and raw format.

Since sharing information is a key component to the voluntary aspect of the critical infrastructure protection and security mission, it is critical that the information provided instills a call to action and enough value to encourage participation towards the goals of the mission. The case study outcomes compared to the CI ISE objective of encouraging action and participation yielded five principles to apply: 1) group-based collection, 2) voting, 3) choosing your own network, 4) direct communication, and 5) casual communication. The DARPA Network Challenge case study revealed that several successful teams with the task of locating the 10 balloons employed direct communication through their networks to promote the cause (helping with the search) and further encouraging additional participants to join in. Other teams took advantage of the voting features within information-sharing environments, such as Facebook, to promote their messages and strengthen the visibility of their content. The Rio de Janeiro case study showed Secretary Costin capitalizing on direct communication to show action based on the information she received, and in return, garner more participation through validation of the process. The Rio case also took advantage of the create your own network principle by creating a completely voluntary network willing to engage and work on improvements. This principle was, in turn, magnified by group-based collection in that

the voluntary network was put to work to improve the curriculum, and provide curriculum guides and tools to teachers and students. A similar combination of principles applied in the CI ISE would yield similar results. As the network of the CI ISE grew and expanded with the use of the choose your own network principle, the other principles—such as group-based collection—could be applied to encourage, promote, and facilitate calls to action.

To meet the overarching goal of providing valuable information in the CI ISE, content must be diverse enough to appeal to the requirements, needs, and perspectives of the very expansive critical infrastructure community. This community is comprised of different disciplines and occupations, is representative of private and public stakeholders, expands across the United States and abroad, and includes organizations of all sizes. Related, the information must be specifically relevant to each facet of the diverse stakeholder set. Both aspects—diverse and relevant—can be mapped to three outcomes of the Rio de Janeiro case study, and the group-based collection and dynamic-content editing. To populate the new Educapedia with content that would appeal to students, teachers, other education personnel and parents, experienced teachers were selected to contribute collectively into the environment employing both principles. The CI ISE already consists of the diverse stakeholder sets. Leveraging that diversity and expertise using the same principles of group-based collection and dynamic-content editing would ensure that the information contributed is diverse (as it comes from diverse points of view and perspectives) and that the information is relevant at least to the stakeholder set the contributor represents, if not more.

It should be noted that the CI ISE characteristic for intelligence products to provide predictive information, as opposed to only reactive information, did not have a companion outcome from the case studies, which may be because none of the case studies included intelligence information sharing, which can be specific and a specialty area. Moreover, the direct lack of outcome from a social media principle may be an indication that social media principles are not poised to correct the deficiency of predictive intelligence information.

2. Information Delivery

In addition to ensuring that the content delivered via the CI ISE is valuable, it is also critical how the information is transmitted. Information delivery is a main focus area of the CI ISE. Presently, the CI ISE has several official mechanisms for sharing information but a common criticism of the GAO and NIAC was that these mechanisms are not integrated, and are often redundant. Stakeholders are burdened to look for information in multiple places and often must rely on finding the information proactively, as opposed to a push or discovery model. The following section describes the case study outcomes and driving principles that have been mapped to improving information delivery.

The information within the CI ISE is expected to be free flowing to ensure information is received from and contributed into the environment without undue process, delay, or administrative burden. Six outcomes across all three case studies mapped to four principles that support free flow of information. The DoS eDiplomacy suite provides resources for subject matter expertise and real professional experiences without overhead of publishing (professional authors, editors, etc.). The tools are enabled by the dynamic content editing principle to allow users to contribute and edit directly, as well as have their contributions instantly included in the environment. Rio de Janeiro and DARPA's use of Twitter allowed for direct communication; in other words, receiving information from stakeholders to organizers instantly. In return, information was shared instantly outward to the network and was directly delivered to those users' information streams. eDiplomacy takes advantage of direct communication also, which included messaging and chat capabilities in the Corridor. Direct communication and dynamic content editing, along with single author content and casual communication, will afford the CI ISE the same opportunity to encourage the free flow of information as seen in these case studies. These principles share the commonality of not requiring formal publishing or review cycles to introduce content into the environment.

The objective to provide meaningful and valuable content to the CI ISE stakeholders leads to a requirement to ensure that content is organized in such a way that stakeholders are not overwhelmed, can find or discover information intuitively and

quickly, and that information can be manipulated in such a way that stakeholders can navigate the environment unique to their requirements and information needs. Five outcomes between the DARPA Network Challenge and DoS's eDiplomacy name dynamic content editing, group-based collection, and tagging as principles affecting these outcomes. Specific to tagging, DARPA Network Challenge teams leveraged tagging features in forums, such as Twitter and Facebook, to ensure that contest participants could filter the conversations and receive direct updates on the contest progress as it unfolded. Likewise, the tagging principle ensured that a large magnitude of information returned from participants was sortable by the organizers. Tagging help eliminate "noise" on the network as well. The CI ISE strives to have the content of multiple varieties (per objectives within improving the value of content), and would immensely benefit from a robust tagging principle application throughout the environment. As with the case studies, tagging will enable filtering to make following conversations or finding content around particular themes easy and manageable. It will also help operation centers, like NICC, that use the environment to receive infrastructure reports, suspicious activity reports, and other similar incoming information feeds.

Central to the criticism of both the GAO and NIAC was the multitude of information sources and platforms from which critical infrastructure stakeholders are expected to visit or monitor to receive information appropriately. While all three case studies demonstrate the utility in having integrated platforms and systems to stitch together a comprehensive information sharing environment, the DoS eDiplomacy case study most illuminates the potential of using social media principles to ensure information is available from multiple entry points in the environment. Leveraging tagging, group-based collection, and dynamic content editing throughout each eDiplomacy suite tool, users are able to find information from one area and use it, promote it, edit it, or add to it from other areas in the site. Moreover, linking user accounts with personal user profiles, content and stakeholders are easily connected throughout the environment. Using the same principles, especially personal user profiles and tagging, the CI ISE can realize a similar synergy throughout the environment. For example, an "active shooter" tag would link training materials, outreach strategies, and

incident reports from several information portals within HSIN-CI. The next chapter provides information on the technology contingencies.

3. Expanding the Reach

With content that is valuable and delivered easily, the next logical objective of the CI ISE is to ensure that the environment is inclusive of the totality of stakeholders who represent the critical infrastructure protection and security mission community. This overarching objective includes the appropriate diversity of stakeholders, trusted and vetted community members, as well as a deep penetration into the critical infrastructure stakeholder set. All three case studies demonstrate using social media principles to manage their community of contributors and consumers. Choose your own network was the most cited principle in outcomes that demonstrated reaching appropriate audiences. DARPA Network Challenge teams relied on reaching a large number of people capable of either inviting additional contest participants or locating and reporting on the balloon location. The only likely unwanted participants were those on competitor teams, capable of misinformation towards opposing team efforts or sharing information with competitors. To achieve maximum participation, these teams leveraged existing social media platforms with networks built from the choose your own network. In most cases, the social media platforms leveraged were public. By contrast, both the DoS eDiplomacy suite and the Rio de Janeiro education reform case studies leveraged the same principle—choose your own network—but within a closed environment. eDiplomacy is mainly purposed for the unique stakeholder set of Foreign Service officers and the Rio de Janeiro education reform efforts looked to target teachers for private (non-public) collaboration on school curriculum and other matters. The principle would benefit the CI ISE in a similar manner, in that sharing information with the public is generally not the goal, and the environment should be networked by practitioners, security personnel, public servants, and other specific stakeholder sets of the critical infrastructure mission.

Six outcomes in the case studies related to diverse participation. Ensuring a diverse stakeholder set in the CI ISE may also be achieved with the help of choose your own network, in which “friends of friends” make for a exponential exposure level for the

community. In addition to choose your own network, the personal user profile principle makes individual network demographics and expertise transparent to the community. The DoS eDiplomacy suite, cataloging all the community members, employed this principle and made them discoverable based on attributes in their profile.

As described in earlier chapters, the critical infrastructure mission requires sensitive information be shared between public and private stakeholders. While safeguards are in place to protect information, a key element to ensuring information is appropriately shared with only the appropriate members of the community; maintaining a trusted and vetted community of stakeholders in the CI ISE is of significant priority. As many as 10 outcomes across all three case studies related to the goal of a trusted network. The 10 outcomes employed the dynamic content editing, personal user profile, choose your own network, and direct communication principles to create an environment in which users were known and their contributions transparent. Of the four principles, choose your own network was most notable in these case studies. In the DoS's eDiplomacy suite, this principle connected professionals in the Foreign Service field virtually and promoted opportunities for knowledge transfer and professional assistance within the network. In Rio de Janeiro's education reform case, this principle afforded an open-minded, willing audience inclusive of teachers, the public, administrators, and students. Just as with the reaching an expanded and deeper audience objective, the CI ISE will benefit from employing the choose your own network principle to connect professionals within the environment, particularly those already connected offline. This objective likely cannot be met with the social media principles alone, however. As discussed in Chapter III, governance and structure will still be at play in the CI ISE to ensure, in this case, appropriate membership.

4. Achieving Multi-Directional Collaboration

The CI ISE doctrine is clear that the environment to support the critical infrastructure information-sharing mission must account for information to flow in multiple directions and that the most productive environment will facilitate collaboration

from all stakeholders.[174] Stakeholders in the CI ISE should be able to participate as both consumers and contributors. Presently, almost all the contributions to the CI ISE are made by the public sector, and more specifically, the DHS. Content is desired to be sourced from all stakeholder types. The environment should allow for coordination of both steady state, such as plans strategies, best practices and protective measures, and on efforts of response and recovery.

Each case study included networks that successfully had stakeholders contributing, as well as consuming. The direct communication and dynamic content editing were the most common principles used in the 10 outcomes related to this objective. Direct communication allowed DARPA Network Challenge teams to both energize and keep their populous up-to-date on progress but also afforded a direct reporting feedback to the organizers over the same medium over which they used to share. Likewise, Rio de Janeiro education reform directly communicated with the entire network to elicit participation in the collaboration happening in other formats across the reform enterprise. To ensure content is sourced from a diverse stakeholder set, the dynamic content editing principle was the most prevalent in related case study outcomes. Diplopedia , of DoS's eDiplomacy, employs this principle to welcome contribution from any member of the community. Few roles exist in the governance of Diplopedia , which ensures that everyone has an opportunity to contribute. Similarly, Educopédia welcomes contributions from all stakeholders, who include teachers, administrators, and students. The CI ISE would see similar contributions to the environment if direct communication were used to engage the stakeholder set. Stakeholders would also likely participate in exercises that employed dynamic content editing as well. More detail on how these can be specifically incorporated is included in the next chapter.

The ultimate utility of the CI ISE is to share information around incidents and events, in either real-time or steady state. Twelve outcomes in the case studies reviewed achieved similar levels of collaboration that would mirror what is desired in the CI ISE. Crowdsourcing was the most prevalent principle in the DARPA Network Challenge, and

[174] Department of Homeland Security, *Critical Infrastructure Key Resources Information Sharing Environment White Paper*.

with a large, geographically disperse problem set, such as finding the 10 balloons across the country, it was the perfect application to receive input quickly and from many different sources. A similar approach could be taken with certain projects within the CI ISE, such as ideas for best practices around a particular theme. In an incident, the crowdsourcing can help pull resources and understand status of various infrastructure affected. Similarly, group-based collection was used in the Rio de Janeiro education reform case study to have a larger set of the teach community contribute to the curriculum, which could be likened to a steady-state plan or policy in the CI IS that needed input from across the critical infrastructure community. Dynamic content editing, as was used in Diplopedia and Educopédia, would assist the CI ISE in an interactive collaboration on a plan or policy as well. As with Educopédia, the CI ISE could use the dynamic content editing to elicit best practices and other resources used among the community into a central repository and location within the environment.

VII. APPLYING SOCIAL MEDIA PRINCIPLES INTO THE CI ISE

Based on the evidence and analysis explained in the preceding chapters, the critical infrastructure information environment can be improved and some of the issues and shortcomings found by the NIAC Intelligence Information Sharing study and others will be addressed by applying social media principles—those features and characteristics that make social media rich with information and networks—to the technologies that support the environment. The evidence and analysis can be summarized into three key findings, which are described in detail in the following section. Putting these principles into place, however, is not without challenge and limitations. This chapter also outlines those impediments and recommends an implementation course of action to overcome those challenges.

A. SUMMARY OF FINDINGS

1. Social Media Principles Utility in CI ISE

The case studies reviewed in this thesis represent a variety of goals intended to be met with information-sharing mechanisms. While none of these goals is specific to homeland security, or the critical infrastructure protection and security missions, they have other attributes in common with the CI ISE. Most notably, these case studies produced outcomes that mirror outcomes expected to be achieved through the CI ISE when the characteristics are well functioning and effective. Also, the case studies applied their social media principles across open and closed environments, which is representative of how critical infrastructure information is to be shared. The evidence and analysis resulting from three cases, their outcomes, related use of social media principles, and ultimate mapping to the CI ISE, suggest that applying the social media principles will have utility in the CI ISE. Further, because many of the characteristics described for the CI ISE in this thesis are documented shortcomings; the principles related to those characteristics may improve the CI ISE when applied in those areas.

Consider that the case studies reviewed in this thesis are only a small sample set of information-sharing problems that have been addressed with the application of modern

information-sharing practices, such as social media. The reviewed case studies had 113 applications that would impact the CI ISE. It is reasonable to conclude that even more evidence would be found that further substantiates the applicability of social media principles to the CI ISE.

2. Social Media Principles Applicability

The three case studies in this thesis produced 41 outcomes. After the outcomes were mapped to the characteristics, 113 social media principle uses emerged as relatable to the case study outcomes, and in turn, to the CI ISE. The social media principles reflected in the 113 uses are representative of 13 social media principles. While most of these principles had applicability in the CI ISE, some emerged as likely more relevant and possible of yielding stronger results in the CI ISE. By contract, one principle—crowdmapping—had no direct relevance to the CI ISE characteristics; however, it is conceivable that this principle would have utility in the CI ISE at a lower ranked objective. Direct communication, with 30 applications across the case studies that mapped to the CI ISE, is the most prevalent principle seen in the analysis. Dynamic content editing and choose your own network were also frontrunners in use, with 21 and 18 uses, respectively. While the remaining principles all were sourced to CI ISE characteristics, these frontrunners may yield a greater "bang for the buck" when applied to the CI ISE because the principles were present for multiple outcomes desired by the CI ISE.

3. Social Media Principles in the CI ISE Do Not Require Public Social Media Technologies.

Due to the nature of the critical infrastructure protection and security and its requirement for secure exchange of information, it is important that any consideration towards applying social media principles does not equate to using public forums to share information. The three case studies presented in this thesis all demonstrated application of the principles distinct from common and well-known social media technologies. The DARPA Network Challenge teams used some public tools, such as Twitter and Facebook, but also took advantage of other less public facing networks.. The Rio de

Janeiro case exemplified using both public social media tools, as well as closed environment solutions. Twitter was a catalyst to starting the conversation and creating the network from which the reform efforts were able to launch more closed conversations and joint efforts. Social media principles were applied to the closed environments, like Educopédia and "Fala, Professor!," to achieve a similar environment to public social media tools. Finally, the DoS eDiplomacy case demonstrated application of social media principles completely within a closed, non-public environment. While the suite of tools mimics popular social media tools, the application of the principles was completely divorced from using public tools. Based on the cased studies' successful application of social media principles absent the use of social media public technologies, the CI ISE can expect to achieve a similar implementation strategy, while maintaining and protecting the integrity and sensitivity of the information in the environment.

As noted in the case study summaries, the case studies used various technologies to employ the social media principles. While the DARPA Network Challenge took advantage of readily available technologies, mostly public networking tools, the DoS built homegrown tools and the Rio de Janeiro case used a mix. This mix of implementation approaches underscores that social media principles, when applied, achieve the information-sharing outcomes desired in the CI ISE, regardless of the technology that employs the principle, including publically accessible technology.

B. IMPEDIMENTS TO THE ADOPTION OF SOCIAL MEDIA PRINCIPLES

1. Culture

Security, intelligence, and law enforcement experts largely manage critical infrastructure. As a generalization, these fields do not culturally share information broadly or publically, as doing so can often compromise the mission of protection. For example, law enforcement agents hold case information close to not taint an investigation, reveal private information about actors in the case, or inadvertently alarm the public. Similarly, security personnel avoid revealing vulnerabilities of their assets or operations so they may not be exploited. Security professionals also share concerns for privacy and public safety, and keeping information protected is critical to ensuring they

are upheld. Social media can be viewed as a vulnerability to these fields in cultures that hesitate to share liberally. Social media is often equated to large public broadcasting mechanisms that violate personal privacy and make it too easy for sensitive material to be leaked or shared with unintended audiences. As described in Chapter 1—Introduction, the distinction between the use of specific social media technology and the principles that make social media successful tools is difficult for those leery of social media in general. Within the security, intelligence, and law enforcement communities, it is fair to characterize that the principles are directly equated to the technology, and therefore, likely to be a challenge to embrace by this stakeholder community.

2. Technology

The principles laid out in the previous chapter require changes to the operations and process of authoring and sharing information, but the key enabler to those principles is technology. Presently, critical infrastructure information sharing relies almost exclusively on the HSIN for electronic distribution and collaboration. This platform is managed by the DHS Office of the Chief Information Officer and recently underwent a major software upgrade.[175] HSIN Release 3 was a technology refresh to a "new, more secure and advanced platform," and while the refresh has reclaimed the tool as the primary information-sharing tool for the department, it is largely still a portal environment.[176] The portal features are similar to those in place when the NIAC and GAO studies were conducted, with most of the changes having occurred in R3, which equated to an upgraded version of Microsoft SharePoint, advanced security and authentication, and new geospatial tools. These welcome improvements do not account for the principles described in this thesis. Adopting them will require additional technologies and new configurations to the HSIN platform.

[175] U.S. Department of Homeland Security, "Homeland Security Information Network," (n.d.), http://www.dhs.gov/homeland-security-information-network; Donna Roy, "DHS Celebrates the Launch of HSIN Release 3," *U.S. Department of Homeland Security*, September 27, 2013, http://www.dhs.gov/blog/2013/09/27/dhs-celebrates-launch-hsin-release-3.

[176] Ibid.

3. Funding

As the current technology employed by the CI ISE does not include many inherent capabilities to employ the social media principles, adjustments to the technology platforms in the form of custom or commercial-off-the-shelf software add-ons will be necessary. The DHS may choose an entirely new software enterprise system with built-in social media capabilities. However, it is reasonable that add-ons or custom adjustments will suffice in converting the current environment. In either case, additional funding will be required to procure the software and finance the engineering labor to integrate. Alternatively, it may reprioritize existing development schedules to replace earlier releases with additional features that align to the social media principles.

The new principles will require adjustments to training plans, standard operating procedures, and other related materials. These adjustments will require funding; however, existing contracts for the CI ISE sector engagement managers to conduct training and adjust materials related to information-sharing processes could be leveraged with the same reprioritization of task approach suggested with the development resources.

4. Policy

The DHS, and likely, many of the organizations represented by stakeholders in the CI ISE have put social media policies in place for the operational use of the media within their organizations. DHS has the *Privacy Policy for Operational Use of Social Media*, which outlines appropriate use of personally identifiable information and related privacy concerns.[177]

The DHS also hosts a comprehensive social media presence across several popular platforms.[178] Generally, these platforms are used for sharing information with the public. Since the current policies of the DHS are geared towards the use of existing, public-facing social media platforms, new policies and governance plans will be required

[177] U.S. Department of Homeland Security, *Privacy Policy for Operational use of Social Media* (Washington, DC: U.S. Department of Homeland Security, 2012).

[178] U.S. Department of Homeland Security, "Social Media Directory," (n.d.), http://www.dhs.gov/social-media-directory.

to outline how the principles within the CI ISE will be used. These policies should provide the same assurances for protection of personal information, as well as other information protection requirements (such as handling of For Official Use Only or protected critical infrastructure information).

C. IMPLEMENTATION

1. Champion

Adopting new information sharing practices will require leadership from within the critical infrastructure community. Leadership will establish new processes and operations to begin the adoption and put the new principles into action. To be sure, as the principles are embraced and integrated, the entire community is expected to participate and perpetuate the impact and power of the principles. However, the process of adoption requires championing the change towards modern information sharing practices.

DHS's Office of IP is responsible for the protection, security, and resilience of the nation's infrastructure. As described in Chapter III, IP manages the policy, governance, processes and technology of the CI ISE. In practice, successful mitigation of risks that face the nation's most critical infrastructure depends on the partnership of state and local governments, and the private sector. However, much of the criticism for the shortcomings in information-sharing practices is directed at the federal government. Additionally, the federal government retains a unique vantage point through its IC, and is typically the first and main source for threat information. Due to these responsibilities, and the directed call for change in the review of current information sharing, the DHS Office of IP is best poised to champion the integration of social media principles in the CI ISE.

In its role as champion, IP must engage the community in the changes and demonstrate commitment to the broader information sharing shortcomings known to the community. By embracing the strategy of applying social media principles in the CI ISE, IP will be putting specific action against the known challenges. The leadership should expect to garner interest and participation from at least some of the community. As more or more progress is observed with implementation, led by IP, the entire endeavor should see a multiplier effect of willing participation.

2. Culture

As described in the impediments section, a current inhibitor to applying modern information sharing techniques like those that seen in social media is the reticence and fear on the part of the critical infrastructure community. To overcome the culture impediment, and succeed at applying social media principles throughout the critical infrastructure information sharing activities, a series of deliberate actions should occur, led by the DHS's Office of IP and reinforced by other DHS offices (such as the Office of Chief Information Officer, Office of Intelligence and Analysis, and the Private Sector Office). The shared actions—a communications strategy, reinforcement of social media, putting principles in practice, and a technology solution—are described in the following sections.

a. Communication Strategy

A communication strategy should be developed to communicate the changes in the information-sharing environment that will be forthcoming. The strategy should clearly articulate the current shortcomings of the environment and include activities to share this assessment with partners. An honest assessment of the current challenges and gaps will appeal to a frustrated audience (who, in many cases, have already identified and documented these shortcomings) and instill confidence that the plans and activities proposed by the government are genuine and have been thoughtfully considered to address the issues and gaps directly. Admitting that the current information-sharing mechanisms are failing the entire community, and that the government is prepared to make the change, will ensure the strategy is taken seriously.

Next, the communication strategy should identify audiences intended to understand the new approaches to information sharing. Among those audiences should be partners that might help reinforce the plans and serve as advocates and evangelists for the change. These partners are ideally private sector organizations that already embrace modern information-sharing practices in their business operations or collaboration with government organizations. They should also understand the current environment and the shortcomings.

Communication should include a comprehensive review of the changes to expect. This review should be simple, itemized, and directly connect the change with intended improvement and outcome. For each principle that will be applied to the environment, the principle should be explained in concept. Then, the principle should be explained in context to illustrate how the principle works in practice and the outcomes other information-sharing environments have achieved when using the principle. Finally, the adjustments to be made to the environment to employ each principle should be explained. In some cases, principles may be employed in multiple places throughout the environment. Each application change should be clearly and simply illustrated to audiences.

Just as important as describing the changes that lay ahead is sharing timelines and schedules for when the changes will occur. Aside from providing predictive expectations, progress, including setbacks, will need to be shared throughout the transformation, which is another area in which transparency will capture loyalty from the intended users of the environment; however, surprises or missed expectations may cause disenfranchisement. Finally, the communications strategy should explain how progress and change would be measured. The plan should include the communication on the measures themselves, as well as reports against the metrics as the implementation and operations progress.

b. Reinforce Social Media

In addition to putting the new principles into action throughout the environment, several tactics and strategies should be simultaneously employed to reinforce the culture shifts. Partnering government agencies should share as much public information as possible through traditional social media, such as Facebook, YouTube, and Twitter. Almost all agencies have at least basic social media presences, but in many cases, they are used for public service information (such as preparing for an emergency). Since these types of applications naturally embody the same principles being introduced to the CI ISE, using them for regular communication will reinforce the practice of these principles, and make them more recognizable and easy to incorporate in the sensitive

information-sharing scenarios. Agencies and organizations should use the applications for more mission-specific information, as opposed to just general public awareness information. For example, a significant campaign at IP is the active shooter training materials and modules. This campaign is designed to help owners, operators, tenants, and employees of critical infrastructure assets prepare for and respond to an active shooter event.[179] The materials are available on the public-facing DHS website. This campaign could be reinforced with Tweets that provide tidbits and facts from the training material that link back to the website. Similarly, the Facebook page could post some status updates with photos from the training that link back to the website. YouTube could be used to play the training videos. Such examples are available throughout the critical infrastructure mission.

3. Put Principles in Practice

Encouraging participation in information sharing is an ongoing challenge for any environment, and the principles of social media alone, will not eliminate the feat. Learning from the case studies, how the government leverages the principles will have a direct impact on the success of their adoption. Like Claudia Costin, the government should respond early and often to every incoming information piece received from a stakeholder. Wherever possible, measurable action should be taken and referenced back to the information received from the partners. In this manner, users are encouraged that their participation in conversations will be fruitful.

One of the biggest criticisms and shortcomings of the current environment is the lack of valuable information. Some of the principles will produce better content through group-based collaboration, and collection and expanded opportunities for more authorship across the networks. However, it will still be necessary for the government to set an example for sharing quality-finished products. The improvements of products themselves are outside the scope of this thesis, but when products are available, they should be provided using as many new principles as possible. For example, a product

[179] U.S. Department of Homeland Security, "Active Shooter Preparedness," (n.d.), http://www.dhs.gov/active-shooter-preparedness.

intends to outline protective measures against a particular set of vulnerabilities. Before the product is finalized, it can be provided in a collaborative space and the environment network for inclusion of best practices from industry. The network can also rate and review the product, and add context of how it was used or helpful.

Finally, IP should host a large collaborative project using the information-sharing environment—with the principles included—to engage the critical infrastructure community in the development of the project. In February 2013, Presidential Policy Directive-21 directed the DHS to update or rewrite the NIPP. This plan, currently in its final stages of draft at the time of this writing, has required extensive collaboration with the critical infrastructure community but it has been almost exclusively "offline." Using the CI ISE and the collaboration principles would not only reach a much broader and more diverse contributor group, but would also allow for efficient collaboration on the document as it evolves through draft stages. While the NIPP is past the stages of requiring collaboration against its drafting, a future collaboration project should be identified to deliberately put the new principles into practice.

4. Technology

Applying social media principles to the CI ISE largely translates to integrating technology features into existing information-sharing mechanisms. Chapter III outlined several mechanisms by which information is shared amongst the critical infrastructure community. Of them, the online network, the HSIN, is the prime mechanism for the application of social media principles. To integrate the principles laid out in the previous chapters fully, the current HSIN technology should be thoroughly evaluated for 1) existing technology features already embedded in the tools that can be configured or used to employ each principle, and 2) opportunities for integrating third-party or newly developed features. Each of these tasks can be undertaken using the existing development and systems engineering staff of the Office of the Chief Information Office (OCIO) in partnership with the HSIN stakeholder engagement mangers within IP. Together, the teams can crosswalk each principle desired against the various elements of the HSIN (portal, document management, web conferencing, etc.) to ensure a configuration is

available. Once an assessment is complete, the engineering teams will integrate either configuration or new development into the regular development and release schedules.

The installation of technology alone is only one step towards truly applying social media principles to the CI ISE. Notably, more important, will be adjusting operating procedures to take advantage of the principles. Using the planning support section of the NICC and the sector outreach and programs division sector engagement managers within IP, standard operating procedures (SOPs) should be reviewed for opportunities to leverage the new principles. Where either a new opportunity exists or an existing process changes with the new principles, SOPs should be updated, socialized, trained against, and exercised.

The HSIN system has been in place for almost 10 years and has been the primary mechanism for sharing information electronically with critical infrastructure stakeholders for most of that time. Integrating the principles of social media into the environment, and specifically, into the HSIN, will require new training for the existing users. They will need to adapt to new processes and procedures for some kinds of sharing but also be enlightened to the new opportunities for participation. Further, the principle of choosing your own network will enlarge the community; in other words, brand new stakeholders will be able to consume and contribute. Consequently, training guides should be updated to explain the new features and operating manuals should be drafted to consider the new opportunities to share information. Exercises hosted by IP should include collaboration elements to practice the principles.

D. MEASURES FOR SUCCESS

Chapter III described four objective areas for the CI ISE: 1) value of content, 2) information delivery, 3) reach, and 4) multi-directional collaboration. The same chapter also listed several specific areas of improvement within each objective area. Recommendations for each area, and in most cases, for each individual objective, are provided in the preceding chapter. After these recommendations are implemented, it will be important to understand and measure how effective the application of each principle

was towards meeting or improving a particular objective. This section outlines four opportunities to monitor and measure the effectiveness of using social media principles in the CI ISE.

The reports describing the current state of critical infrastructure information sharing provide a benchmark for where the current effectiveness of each area stands presently. These benchmarks can be compared to new statuses after implementation. In some areas, more subjective measurement will be required, like in value of content. In those cases, the DHS may ask its council partners (the NIAC or other sector coordinating councils) to re-evaluate their previous findings or provide a fresh perspective on how information is valued in the CI ISE. The updated reports with subjective input from stakeholders can be compared directly to the previous reports.

In other areas, more quantitative measures will be available. Monitoring usership of the technology will yield an understanding of the reach of the CI ISE. Historically, IP collects and monitors statistics for both the HSIN-CI and other information-sharing mechanisms, such as number of participants on incident coordination calls, number of subscribers to the Open Source Infrastructure Report and the number of contacts each field PSA has. In continuation, these statistics can be compared over time as the social media principles are implemented into the CI ISE. A basic growth in number of the HSIN-CI accounts will give a general indication if the network is growing. Subscriptions to email notifications, website updates, and other similar opt-in communication mechanisms will also indicate an improvement in reach. Monitoring other usage statistics may indicate the value users find with the environment. To measure if users are actually logging in and spending time in the environment, sessions can be captured. The amount of time a user spends could be an indication of finding value in the environment; however, this statistic cannot be relied on alone. The length of time could indicate trouble finding material, a current shortfall. Additional context will be needed from surveys or other overlaid subjective information, aside from membership alone.

Aside from quantitative measures like statistics, information-sharing practices can be observed and reflected upon during and after real-life scenarios in which the mechanisms are stressed for utility. Typically, significant incidents are reviewed in after

action reports or "hot washes," and commonly, a thorough review of how information flowed and what was available to whom and when is central to these after-action activities. In addition to real-life events, exercises are common within the critical infrastructure community. Whether the exercise is directly targeted at practicing information-sharing processes, because information sharing is so central to achieving any part of the critical infrastructure protection and security mission, any exercises will allow for observation on the CI ISE environment and the four area objectives. As with real-life incidents, exercises include after-action surveys, discussions, and reports to understand what worked well and what areas need improvement.

Finally, to address the subjective nature of evaluating the CI ISE, and in turn, the effectiveness of the social media principles applied to the environment, surveys (or interviews) conducted throughout the community will yield an understanding of the stakeholders' direct perception of the environment and its improvement over time.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York, NY: Penguin, 2006.

Bratton, William, and Zachary Tumin. *Collaborate Or Perish!: Reaching Across Boundaries in a Networked World*. New York, NY: Random House Digital, 2012.

Brisbane City Council. "Brisbane Storm and Flood Map." (n.d.). https://bnestorm.crowdmap.com/main).

Bronk, Chris, and Tiffany Smith. "Diplopedia Imagined: Building State's Diplomacy Wiki." In *Proceedings of the 2010 International Symposium on Collaborative Technologies and Systems*. Chicago, IL: IEEE, 2010. http://bakerinstitute.org/files/824/.

Bruns, Barbara, David Evans, and Javier Luque. *Achieving World-Class Education in Brazil: The Next Agenda*. Washington, DC: World Bank, 2011.

Burke, Wayne Moses. "GovLuv." In *The Big Book of Social Media*, edited by Robert Fine. Tulsa, OK: Yorkshire Publishing, 2010.

Chertoff, Michael. *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security (DHS), 2009.

CNN.Com. "MIT Wins $40,000 Prize in Nationwide Balloon-Hunt Contest." December 7, 2009. http://www.cnn.com/2009/TECH/12/05/darpa.balloon.challenge/index.html?_s=PM:TECH.

Crowdsourcing. "Crowdsourcing: A Definition." June 2, 2006. http://crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html.

Defense Advanced Research Projects Agency. *DARPA Network Challenge Project Report*, 2010.

Delicious. "About Us." (n.d.). https://delicious.com/about.

Educopédia. "Educopédia." (n.d.). http://www.educopedia.com.br0/SobreEducopedia.aspx.

Ellison, Nicole B. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210–230.

Executive Order 13549: Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities. College Park, MD: Office of the Federal Register, National Archives and Records Administration, 2010.

Facebook Newsroom. “Key Facts.” 2013. http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

Giles, Jim. “Internet Encyclopaedias Go Head to Head.” *Nature* 438, no. 7070 (2005): 900–901.

Golder, Scott, and Bernardo A. Huberman. “Usage Patterns of Collaborative Tagging Systems.” *Journal of Information Science* 32, no. 2 (2006): 198–208.

Hammond, Tony et al. “Social Bookmarking Tools (I) a General Review.” *D-Lib Magazine* 2, no. 4 (2005).

Hanson, Fergus. *Revolution@ State: The Spread of eDiplomacy*. Sydney NSW 2000 Australia: Lowy Institute for International Policy, 2012.

ISE.Gov. “Information Sharing Partnerships with the Private Sector—Owners of 85% of the Critical Infrastructure in the US.” (n.d.). http://www.ise.gov/mission-partner/critical-infrastructure-and-key-resources.

Kaplan, Andreas M., and Michael Haenlein. “Users of the World, Unite! The Challenges and Opportunities of Social Media.” *Business Horizons* 53, no. 1 (2010): 59–68.

Moteff, John, and Paul Parfomak. *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report RL32631. Washington, DC: Library of Congress, Congressional Research Service, October 1, 2004.

National Infrastructure Advisory Council. *Intelligence Information Sharing*, 2012.

Nielsen Company, The. “State of Media: The Social Media Report.” December 4, 2012. http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf.

O’Reilly, Tim. “What Is Web 2.0.” *O’Reilly Media*, 2005. http://oreilly.com/web2/archive/what-is-web-20.html.

OECD. “OECD Programme for International Student Assessment (PISA).” (n.d.). http://www.oecd.org/pisa/.

———. “Organisation for European Economic Co-Operation.” (n.d.). http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm.

———. “Organisation for Economic Co-Operation and Development.” 2013. http://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm.

Roy, Donna. “DHS Celebrates the Launch of HSIN Release 3.” *U.S. Department of Homeland Security*, September 27, 2013. http://www.dhs.gov/blog/2013/09/27/dhs-celebrates-launch-hsin-release-3.

SelectUSA. “The Retail Services Industry in the United States.” (n.d.). http://selectusa.commerce.gov/industry-snapshots/retail-services-industry-united-states.

Smith, Aaron. “Why Americans Use Social Media.” *Pew Research Center,* November 15, 2011. http://www.pewinternet.Org/Reports/2011/Why-Americans-use-Social-Media.Aspx.

Surowiecki, James. *The Wisdom of Crowds*. New York, NY: Random House Digital, Inc., 2005.

Transportation Security Administration. “Sensitive Security Information (SSI).” (n.d.). http://www.tsa.gov/stakeholders/sensitive-security-information-ssi.

Twitter Stats. “Popular Apps and Tweets.” (n.d.). http://tweetstats.com/twitter_stats; Facebook Newsroom. “Key Facts.”

———. “TweetStats.” 2013. http://www.tweetstats.com//twitter_stats.

U.S. Department of Homeland Security. “Active Shooter Preparedness.” (n.d.). http://www.dhs.gov/active-shooter-preparedness.

U.S. Department of Homeland Security. “Chemical-Terrorism Vulnerability Information.” (n.d.). http://www.dhs.gov/chemical-terrorism-vulnerability-information.

———. “Critical Infrastructure Partnership Advisory Council.” (n.d.). http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

———. *Critical Infrastructure Information Sharing Environment*. Washington, DC: U.S. Department of Homeland Security, 2012.

———. *Critical Infrastructure Key Resources Information Sharing Environment White Paper*. Washington, DC: U.S. Department of Homeland Security, 2012.

———. “Homeland Security Information Network.” (n.d.). http://www.dhs.gov/homeland-security-information-network.

———. *HSIN-CS Usage Statistics*. Washington, DC: U.S. Department of Homeland Security, 2012.

———. *Privacy Policy for Operational use of Social Media*. Washington, DC: U.S. Department of Homeland Security, 2012.

———. “Protected Critical Infrastructure Information (PCII) Program.” (n.d.). http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

———. *Quadrennial Homeland Security Review*. Washington, DC: U.S. Department of Homeland Security, 2010.

———. "Social Media Directory." (n.d.). http://www.dhs.gov/social-media-directory.

U.S. Department of State. "About: Diplopedia ." October 12, 2012. http://www.state.gov/m/irm/ediplomacy/115847.htm.

———. "IRM's Office of eDiplomacy." (n.d.). http://www.state.gov/m/irm/ediplomacy/.

———. "Major Programs of IRM's Office of eDiplomacy." (n.d.). http://www.state.gov/m/irm/ediplomacy/c23840.htm.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors Characteristics : Report to Congressional Requesters*. GAO-07-39. 2006.

———. *Public Transit Security Information Sharing*. GAO-20-895. 2010.

———. *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*. GAO-11-688T. 2011.

Ushahidi. "Ushahidi." (n.d.). http://ushahidi.com/; Official Blog. "Google+: Communities and Photos." December 6, 2012. http://googleblog.blogspot.com/2012/12/google-communities-and-photos.html.

Vickery, Graham, and Sacha Wunsch-Vincent. *Participative Web and User-Created Content: Web 2.0 Wikis and Social Networking*. Paris, France: Organization for Economic Cooperation and Development (OECD), 2007.

White House, The. "Presidential Policy Directive—Critical Infrastructure Security and Resilience." February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

———. "Sharing Information with the Private Sector." (n.d.). http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionV.html.

Wikipedia, s.v. "1998 United States Embassy Bombings." Last modified November 27, 2013. http://en.Wikipedia.org/wiki/1998_United_States_embassy_bombings.

———. "About." Last modified November 27, 2013. http://en.Wikipedia.org/wiki/Wikipedia:About.

———. "Crowdsourcing." Last modified November 28, 2013. http://en.Wikipedia.org/wiki/Crowdsourcing.

———. “Geocaching.” Last modified November 19, 2013. http://en.Wikipedia.org/wiki/Geocaching.

———. “Office of eDiplomacy.” Last modified November 20, 2013. http://en.Wikipedia.org/wiki/Office_of_eDiplomacy.

———. “Social Bookmarking.” Last modified October 29, 2013. http://en.Wikipedia.org/wiki/Social_bookmarking.

———. “Web 2.0.” Last modified November 28, 2013. http://en.Wikipedia.org/wiki/Web_2.0.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California